VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA PRÁVA

Využití elektronického podpisu na okresním soudě
Electronic Signature Aplication at Regional Court

Student: Bc. Ondřej Kyčerka
Vedoucí diplomové práce: Mgr. Bc. Adam Ptašnik, Ph.D.

Ostrava 2011

VŠB-Technická univerzita Ostrava | Ekonomická fakulta
Katedra práva | Akademický rok 2010/2011

Zadání diplomové práce

Student: Bc. Ondřej Kyčerka

Studijní program: Ekonomika a management

Studijní obor: Ekonomika a právo v podnikání

Téma: Využití elektronického podpisu na okresním soudě
Aplication Electronic Signature at Region Court

1. Úvod
2. Teoretická východiska využití elektronického podpisu
3. Právní úprava elektronického podpisu
4. Využití elektronického podpisu v praxi
5. Závěr
Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Přílohy

Seznam doporučené odborné literatury:

BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. 141 s. ISBN 80-7263-125-X.

BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. 157 s. ISBN 978-80-7263-465-1.

ZELENKA, J. a kol. *Ochrana dat: kryptologie.* 1.vyd. Hradec Králové: Gaudeamus, 2003. 198 s. ISBN 80-7041-737-4.

Vedoucí diplomové práce: Mgr. Bc. Adam Ptašnik, Ph.D.

Datum zadání: 26. listopadu 2010

Datum odevzdání: 29. dubna 2011

JUDr. Bohuslav Halfar
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

„Místopřísežně prohlašuji, že jsem celou diplomovou práci, včetně všech příloh, vypracoval samostatně a uvedl jsem veškerou použitou literaturu a další prameny.“

Ostrava 29. dubna 2011

Bc. Ondřej Kyčerka

Obsah

1. Úvod

Téma Využití elektronického podpisu na okresním soudě jsem si vybral, neboť mě toto téma zajímá a nebylo doposud nikde řešeno. Prostřednictvím této práce bych chtěl přinést vlastní pohled na danou problematiku.

Hlavním cílem diplomové práce je zhodnotit úroveň využití elektronického podpisu na Okresním soudě v Ostravě, prostudovat právní úpravu elektronického podpisu, která je nezbytná pro správné užívání elektronického podpisu v této instituci a zanalyzovat samotné využití elektronického podpisu v praxi.

Tato diplomová práce je rozdělena do pěti kapitol. Po krátkém úvodu následuje kapitola zabývající se teoretickými východisky využití elektronického podpisu. Kapitola se zabývá základními pojmy, jejichž znalost je nezbytná pro pochopení této diplomové práce. Blíže jsou vysvětleny pojmy jako: elektronický podpis, veřejná správa, e-Government, elektronická podatelna, datové schránky, certifikáty, certifikační autorita, kvalifikovaná certifikační autorita a časové razítko.

Právní úprava elektronického podpisu je vysvětlena ve třetí kapitole. Zde bude především detailně rozebrán zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů. Posléze je věnována pozornost nařízení vlády č. 495/2004 Sb., kterým se provádí zákon o elektronickém podpisu; vyhlášce č. 496/2004 Sb., o elektronických podatelnách a v neposlední řadě vyhlášce č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. Zmíněn bude rovněž zákon č. 40/1964 Sb., občanský zákoník. Závěrem této kapitoly se čtenář seznámí se směrnicí 1999/93/EC Evropského parlamentu a Rady o zásadách společenství pro elektronické podpisy. Znalost výše zmíněných právních předpisů je nezbytná pro správné užívání elektronického podpisu na Okresním soudě v Ostravě, což jen podtrhuje důležitost této kapitoly.

Čtvrtá kapitola se zaměřuje na využití elektronického podpisu v praxi. V této kapitole bude věnována pozornost následujícím tématům: využití ePodatelny soudy; Pravidla pro zajištění provozu ePodatelny na Okresním soudě v Ostravě; Postup Okresního soudu v Ostravě při komunikaci prostřednictvím datové schránky; Vydávání certifikátů od společnosti Česká pošta, s. p a rovněž jsou zde zmíněny potenciální problémy spojené s elektronickým podpisem.

V rámci výše zmíněné kapitoly jsem provedl analýzu využití elektronického podpisu na Okresním soudě v Ostravě prostřednictvím dotazníkového šetření. Předmětem analýzy je aplikovaný výzkum exploračního typu formou dotazníkového zkoumání zaměřeného na úroveň využití elektronického podpisu v organizaci veřejné správy. Objektem šetření jsou zaměstnanci Okresního soudu v Ostravě.

Význam dotazníkového šetření spočívá v nalezení odpovědí na předem vybrané otázky, ze kterých se následně pokusím vypracovat návrhy a doporučení pro zkvalitnění úrovně využití elektronického podpisu na Okresním soudě v Ostravě.

V samotném závěru práce jsem komplexně shrnul obsah této diplomové práce. Uvedl podstatná zjištění, která vyplynula z dotazníkového šetření, a nastínil možná doporučení, jež by vedla ke zlepšení stávajícího stavu.

2. Teoretická východiska využití elektronického podpisu

V této kapitole se čtenář seznámí se základními pojmy, jejichž znalost je nezbytná pro pochopení této diplomové práce. Blíže budou vysvětleny pojmy jako: elektronický podpis, veřejná správa, e-Government, elektronická podatelna, datové schránky, certifikáty, certifikační autorita, kvalifikovaná certifikační autorita a časové razítko.

Dnešní doba je ovlivněna neustálým pokrokem výpočetních technologií, které nabízí široké možnosti jak zefektivnit a usnadnit práci a komunikaci. Elektronizace přináší do našeho života mnoho nového. Některé věci, známé a užívané v každodenním životě, získávají i svou elektronickou podobu. Jednou z těchto technických vymožeností je bezesporu elektronický podpis, který ve své podstatě lze chápat jako obdobu vlastnoručního podpisu.[1]

Elektronický podpis nachází využití především při komunikaci osoby s celou řadou institucí. Jsou jimi např. zdravotní pojišťovny, krajské, městské a obecní úřady. Využívá se při komunikaci se soudy, při podepisování faktur a emailových zpráv, u žádostí o sociální a rodičovské dávky, u podávání přihlášky a odhlášky k nemocenskému pojištění a mnoho jiných.

Z obecného hlediska je elektronický podpis souborem digitálních dat, kterými podepisující osoba vytváří pomocí svého soukromého klíče digitální podpis a zajišťuje jimi nepopiratelnost původu (identifikaci) podepsaných dat v prostředí internetu.[2]

[1] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 7 ISBN 978-80-7263-465-1.
[2] *Internetové stránky PRO Consluting*. Dostupný z WWW: <http://www.proconsulting.cz >. [citováno 2011-03-02].

2.1 Základní pojmy

V současné době začíná u nově vznikajících předpisů a dokumentů převažovat elektronická forma. Postupně stále více právních předpisů přechází z tradiční do elektronické formy a umožňuje používání elektronického podpisu v oblasti orgánů veřejné správy, a to jak při komunikaci mezi úřady navzájem, tak při komunikaci občanů s jednotlivými, výše zmíněnými úřady.[3]

2.1.1 Elektronický podpis

Synonymem pojmu elektronický podpis se rozumí digitální podpis, či zaručený elektronický podpis (dále jen elektronický podpis). Elektronický podpis je zpravidla chápán jako číslo, které vytváří podepisující osoba dle svých dat pro tvorbu elektronického podpisu a pomocí zprávy, kterou podepisuje. [4]

Principem podepisování je připojení určitého identifikátoru. Tímto identifikátorem může být heslo; obraz; otisk prstu či ruky.[5] Elektronický podpis může být i podpis, který je napsán z klávesnice počítače, ten však nevzbuzuje velkou důvěru. Je těžké identifikovat a prokázat kdo jej skutečně psal.

V případě, že zpráva byla podepsána zaručeným elektronickým podpisem pak

- podepisující osoba, která zprávu podepsala, nemůže popřít, že je jejím původcem
- je možné zjistit, zda zpráva nebyla změněna poté, co byla podepsána
- lze zjistit identitu podepsané osoby
- je zajištěna právní akceptovatelnost podpisu

Výše uvedených vlastností může využít kdokoliv, kdo se na daný podpis spoléhá.

---

[3] *Internetové stránky Ministerstva vnitra ČR.*. Dostupný z WWW: <http://www.mvcr.cz >. [citováno 2011-03-02].

[4] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. s. 129 ISBN 80-7263-125-X.

[5] SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systémů*. 2.vyd.Praha: C.H.Beck, 2004. s. 84 ISBN 80-7179-765-0.

Zaručený elektronický podpis je pokaždé jiný, závisí totiž na textu, ke kterému je připojen a na použitých datech při jeho vytváření.[6] V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen „uznávaný elektronický podpis“). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám.

V případě, že je uznávaný elektronický podpis používán v oblasti orgánů veřejné moci, je nezbytné, aby kvalifikovaný certifikát obsahoval takové údaje, které jednoznačně osobu identifikují.

V případě písemností orgánů veřejné moci v elektronické podobě, označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu, vydaných akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.

Akreditovaným poskytovatelem certifikačních služeb se rozumí poskytovatel certifikačních služeb, kterému byla udělena akreditace dle zákona o elektronickém podpisu. Jestliže poskytovatel hodlá nabízet akreditované certifikační služby v dané zemi, je potřeba aby prošel procesem akreditace právě zde. Akreditace vydaná v jedné zemi není využitelná v druhé zemi. Akreditačním orgánem v České republice byl zpočátku Úřad pro ochranu osobních údajů, posléze Ministerstvo informatiky a v současné době kompetence spojené s elektronickým podpisem přecházejí na Ministerstvo vnitra.[7]

Ministerstvo vnitra udělilo akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb třem subjektům: První certifikační autoritě, a.s.; České poště, s. p. a eIdentity, a.s.

[6] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. s. 129 ISBN 80-7263-125-X.
[7] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 25 ISBN 978-80-7263-465-1.

2.1.2 Využití elektronického podpisu

V souvislosti s využitím elektronického podpisu se můžeme setkat s následujícími pojmy:

- *Soukromý klíč* - soukromým klíčem jsou označována data pro vytváření elektronických podpisů.
- *Veřejný klíč* – veřejným klíčem jsou označována data pro ověřování elektronických podpisů.
- *Hash funkce* – jedná se o matematickou funkci, kterou lze v jednom směru (přímém) snadno spočítat, zatímco v opačném směru (inverzní zobrazení) výpočty probíhají velmi obtížně.

Výsledkem hash funkce je několik desítek či stovek bitů dlouhá sekvence jednoznačně charakterizující vstupní blok dat. Vstupní informací pro hash funkci v případě elektronického podpisu je podepisovaný dokument.[8]

K vytvoření elektronicky podepsané a zašifrované zprávy lze využít následující postup. Odesílatel zprávy nejdříve vypočte hash hodnotu zprávy, kterou zašifruje svým soukromým klíčem, což vede k vzniku elektronického podpisu zprávy. Následně zašifruje zprávu veřejným klíčem adresáta, čímž ji „znečitelní“ pro neautorizované subjekty.

Upravená zpráva je poté společně s elektronickým podpisem předána (odevzdaná na datovém nosiči, zaslaná po síti atd.) adresátovi. Adresát zprávu dešifruje prostřednictvím svého soukromého klíče, čímž se zpráva stane čitelná. Posléze ověří podpis výpočtem hash hodnoty zprávy a jejím srovnáním s dešifrovanou hodnotou z elektronického podpisu.

Jestliže jsou hash hodnoty stejné, elektronický podpis byl vytvořen uvažovanou osobou a zpráva nebyla po jejím podepsání změněna (kontrola integrity zprávy). V případě, že hash hodnoty nejsou shodné, nepovažuje se elektronický podpis za platný a zpráva se stává nedůvěryhodnou.[9] Výše popsaná situace je zobrazena na obrázku 2. 1. na následující straně.

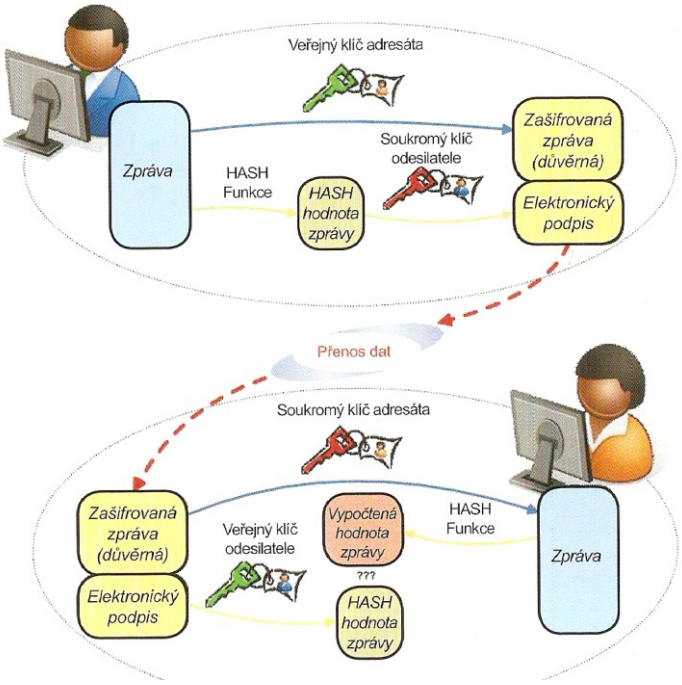
---

[8] *Internetové stránky Ministerstva vnitra ČR.*. Dostupný z WWW: <http://www.mvcr.cz >. [citováno 2011-03-05].

[9] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 35-36 ISBN 978-80-7263-465-1.

Bezpečnost při využití elektronického podpisu je založena na skutečnosti, že nemohlo dojít k narušení tajnosti privátního klíče, nebyl prolomen použitý kryptoalgoritmus ani porušena kryptologická bezpečnost hash funkce a nedošlo ani k porušení autentičnosti veřejného klíče.[10]

Obrázek 2. 1 Bezpečná komunikace s využitím elektronického podpisu



Zdroj: BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vydání. s. 35

2.2 Veřejná správa

Veřejná správa je v České republice vykonávána státem (státní správa) a územně příslušnými samosprávnými celky (samospráva - obce a kraje). Veřejná správa řídí veřejné záležitosti v mezích zákona a způsoby v zákoně povolenými.[11] V současné době občané využívají elektronický podpis vůči orgánům veřejné správy především v oblasti správy daní a v obecných správních řízeních. [12]

[10] ZELENKA, J. a kol. *Ochrana dat: kryptologie.* 1.vyd. Hradec Králové: Gaudeamus, 2003. s. 150 ISBN 80-7041-737-4.
[11] *Portál Regionálních Informačních servisů.* Dostupný z WWW: <http://www.mvcr.cz >. [citováno 2011-03-07].
[12] *Internetové stránky Ministerstva vnitra ČR.*. Dostupný z WWW: <http://www.mvcr.cz >. [citováno 2011-03-07].

2.3 e-Government

Pojem e-Government můžeme chápat jako elektronizaci státní správy a samosprávy. V nejlepším případě jej lze považovat za elektronizaci celého výkonu veřejné moci včetně rozhodovacích procesů. E-Government má význam transformace vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem zefektivnit vnitřní procesy.

Mezi nesporné výhody elektronizace veřejné správy patří především jednoduchost; uživatelská přívětivost; úřední hodiny pro podání 24 hodin denně, 7 dnů v týdnu; finanční úspory a transparentnost procesů a rozhodování.[13]

Cíle e-Governmentu

- Hlavním cílem je rychlejší, levnější a kvalitnější poskytování služeb veřejné správy široké veřejnosti.
- Zvýšení výkonnosti státní správy by mělo přispět ke zjednodušení činností veřejnosti při styku s veřejnou správou.
- Vymezení procesně-správního charakteru činnosti správních úřadů a jeho odrazu ve funkcích informačních systémů, zabezpečení předávání dat
- Vytvořit účelnou elektronizaci vnitřních agend ve veřejné správě, pouze takováto elektronizace v konečném důsledku umožní veřejnosti volbu lokality a možnost způsobu komunikace s veřejnou správou. [14]

Pro rozvoj e-Governmentu je nezbytná legislativní podpora. Úřady nezavedou ani nemohou zavést žádné kroky v oblasti elektronizace bez jasného vymezení v zákonech.

[13] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 20 ISBN 978-80-7263-465-1.
[14] *Internetové stránky Ministerstva vnitra ČR.* Dostupný z WWW: <http://www.mvcr.cz >. [citováno 2011-03-09].

2.3.1. Elektronická podatelna

Zásadním pojmem v oblasti e-Governmentu je elektronická podatelna. Ta je definována v nařízení vlády č. 304/2001 Sb., jako pracoviště pro příjem a odesílání datových zpráv. Dle zmíněného nařízení mají povinnost zřídit jedno či více takových pracovišť orgány veřejné moci, stejně tak samosprávné celky, které provádějí výkon státní správy v rámci přenesené působnosti. Vlastní funkci ePodatelny detailně popisuje vyhláška o elektronických podatelnách č. 496/2004 Sb., vydaná bývalým Ministerstvem informatiky.

Ta stanovuje postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny.[15]

Tzv. ePodatelny musí být vybaveny zařízeními připojenými k veřejné datové síti, či jiným sítím. Tato zařízení musí nejen splňovat technické a programové vybavení, ale také musí umožňovat užívání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, jenž je vydán akreditovaný poskytovatelem.[16]

2.3.2 Datové schránky

Dne 1. července 2009 nabyl účinnosti zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Zákon o e-Governmentu, jak bývá tento zákon označován, upravuje elektronickou komunikaci mezi orgány veřejné moci navzájem a dále upravuje komunikaci právnických osob a orgánů veřejné moci. Za průlom, který přinese značné časové a finanční úspory se považuje, že užívání elektronické komunikace se stává v mnoho případech povinné.

Výše zmíněný zákon předepisuje pro komunikaci použití datových schránek, které se stávají elektronickou obdobou fyzických poštovních schránek. Komunikující subjekty vstupují do schránek pouze bezpečným způsobem prostřednictvím průkazné autentizační a autorizační procedury.

---

[15] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 21 ISBN 978-80-7263-465-1.

[16] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. s. 129 ISBN 80-7263-125-X.

Jakýkoli důležitý úkon spojený časem, tedy zaslání dokumentu do datové schránky komunikačního partnera, přístup do vlastní schránky nebo její vybírání, bude doložen vytvořením kvalifikovaného časového razítka. Datové schránky umožňují užití zaručeného elektronického podpisu přenášených zpráv. Tyto bezpečnostní technologie poskytují stejnou důvěryhodnost a právní váhu jako doručení do vlastních rukou.

Zákon o e-Governmentu vedle datových schránek a elektronického doručování dokumentů řeší i autorizovanou konverzi dokumentů, a to oběma způsoby.

Papírový dokument bude možné převést na elektronický a elektronický dokument na papírový aniž by došlo ke ztrátě právní váhy dokumentu. Tento krok směřuje k rovnocennosti elektronických a papírových dokumentů.

Jestliže dochází ke konverzi elektronického dokumentu do papírové podoby, očekává se, že původní dokument je podepsán zaručeným elektronickým podpisem a opatřen časovým razítkem.

Je jen otázkou času, kdy počet podání elektronickou formou převýší počet podání v písemné podobě. Elektronická komunikace zcela nenahradí osobní návštěvu na úřadech, ale jedná se o cestu nejen jednodušší a rychlejší, ale i levnější. Agenda řešena elektronicky totiž občanům odpouští správní poplatky, což může znamenat úsporu až stovek korun.[17]

2.4 Certifikát

Elektronický podpis umožňuje ověřit, že zprávu podepsal vlastník odpovídajícího soukromého klíče, což však nijak neidentifikuje skutečnou osobu, která daný klíč vlastní. Certifikát slouží právě jako ten nástroj, který umožní spolehlivě identifikovat skutečného odesilatele zprávy.

Certifikát lze přirovnat k občanskému průkazu, neboť občanský průkaz spojuje identifikační údaje s jedinečným identifikátorem konkrétní osoby, kterým je její podoba (reprezentovaná fotografií). Co se týče certifikátu, tímto identifikátorem je veřejný klíč.[18]

[17] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 25-26 ISBN 978-80-7263-465-1.
[18] DOLEŽAL, Dušan. Co to je digitální certifikát. *E-komerce* [online]. 2003 [cit. 2011-03-20]. Dostupný z WWW: <http://interval.cz/clanky/co-to-je-digitalni-certifikat/>.

Certifikát slouží k spolehlivému a věrohodnému předání dat pro ověřování elektronického podpisu podepisující osoby. Certifikátem se rozumí datová zpráva, která je vydávána poskytovatelem certifikačních služeb. Spojuje data sloužící k ověření elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu. Případně spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její totožnost.[19]

Certifikáty ve své nejjednodušší formě obsahují:

- veřejný klíč
- jméno a další údaje zajišťující jednoznačnou identifikaci subjektu, kterému byl certifikát vydán
- datum počátku platnosti a datum ukončení platnosti certifikátu
- jméno certifikační autority, která certifikát vydala
- sériové číslo[20]

Zákon č. 227/2000 Sb. o elektronickém podpisu upravuje předávání dat pro ověřování elektronického podpisu pouze prostřednictvím kvalifikovaných certifikátů. V praxi jsou však užívány i jiné způsoby, či certifikáty, které kvalifikované nejsou ve smyslu zákona o elektronickém podpisu. Certifikáty jako způsob předávání dat pro ověřování elektronického podpisu používá Microsoft Outlook, či Outlook Express.[21]

Certifikát, který je vydán kvalifikovaným poskytovatelem certifikačních služeb se nazývá kvalifikovaný certifikát. Jestliže má certifikát být použitelný například pro podávání žádosti na úřadě, musí být vydaný akreditovaným poskytovatelem certifikačních služeb.[22]

---

[19],[21] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. s. 123 ISBN 80-7263-125-X.

[20] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 39 ISBN 978-80-7263-465-1.

[22] *Příručka o elektronickém podpisu* [online]. 2007 [cit. 2011-03-15]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/micr/files/3908/pririicka_el_podpis.pdf/>.

Kvalifikovaný certifikát, o který žádají orgány státní správy, má nevýhodu v tom, že může být použit pouze za účelem podepisování dat, zatímco komerční certifikát může být použit i pro jejich zašifrování.

Vlastníkem certifikátu je fyzická osoba, právnická osoba či organizační složka státu, která požádala o vydání kvalifikovaného certifikátu pro sebe nebo pro podepisující osobu a které byl certifikát následně vydán. Z výše uvedeného vyplývá, že ten, kdo je podepsán, nemusí být držitelem certifikátu.

V praxi se hovoří o tzv. zaměstnaneckých certifikátech, které pro své zaměstnance pořizuje zaměstnavatel. Zaměstnanec prostřednictvím svého soukromého klíče může jednat jménem svého zaměstnavatele a v případě jeho odchodu může zaměstnavatel certifikát zneplatnit.[23]

2.4.1 Certifikační autorita

V zákoně o elektronickém podpisu je certifikační autorita (CA) definována jako fyzická osoba, právnická osoba nebo organizační složka státu. V rámci své činnosti CA vydává certifikáty, vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy. Tato autorita je důvěryhodným zdrojem jak pro podepisující osoby, kterým certifikáty vydává, tak pro osoby, které se na podpisy spoléhají.

Certifikační autorita vystupuje při vzájemné komunikaci dvou subjektů jako třetí, nezávislý subjekt, který prostřednictvím vydaného certifikátu svazuje identifikaci subjektu s jeho dvojící klíčů, respektive s jeho elektronickým podpisem.[24]

Poskytovatel certifikačních služeb vydává certifikáty, za určených podmínek je zneplatňuje a vydává CRL – seznam zneplatněných certifikátů.[25]

---

[23] *Příručka Certifikační autority PostSignum* [online]. 2010 [cit. 2011-03-16]. Dostupný z WWW: <http://www.postsignum.cz/files/navody/CA_P54_zakaznik_PO_PFO.pdf/>.

[24] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace.* 1. vyd. Olomouc: ANAG, 2008. s. 39 ISBN 978-80-7263-465-1.

[25] CRL je dokument, kde jsou uvedeny neplatné certifikáty, jejichž běžná doba platnosti ještě nevypršela. CRL je podepsán poskytovatelem a je veřejně přístupný. Certifikáty jsou zde uvedeny do doby, než jejich platnost řádně vyprší.

Certifikační autorita může vydávat certifikáty prostřednictvím určeného subjektu či některé činnosti zajišťovat prostřednictvím služby registračních autorit, vždy však zůstává odpovědná za poskytované služby.[26]

2.4.2 Kvalifikované certifikační autority

V České republice jsou tři kvalifikované certifikační autority, které získaly akreditaci Ministerstva vnitra. Jsou jimi:

Česká pošta, s. p. – ta se stala akreditovaným poskytovatelem certifikačních služeb dne 3. 8. 2005 na základě rozhodnutí Ministerstva informatiky (nyní v kompetenci Ministerstva vnitra).[27]

eldentity, a.s. – vznikla počátkem roku 2004 s cílem orientovat se na komplexní služby v oblasti elektronické identity. Společnost získala v září roku 2005 akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb.

První certifikační autorita, a.s. (zkr. I. CA) - zahájila poskytování svých služeb v roce 1996 jako součást projektu společnosti PVT, a.s. Postupně I. CA přerostla hranice projektu a v roce 2001 vznikla dceřiná společnost PVT, a.s. s názvem První certifikační autorita, a.s. Tehdejší akreditační orgán - Úřad pro ochranu osobních údajů udělil První certifikační autoritě, a.s. akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu s účinností od 18. 3. 2002. I. CA takto úspěšně ukončila akreditační proces a je oprávněna poskytovat služby v oblasti kvalifikovaných certifikátů.

V současnosti je I. CA největším poskytovatelem komplexního servisu vydávání a správy certifikátů v České republice. Od roku 2006 společnost poskytuje kvalifikované systémové certifikáty a kvalifikovaná časová razítka. Pro zajištění realizace požadavků svých klientů provozuje I. CA infrastrukturu tzv. registračních autorit.

Tato kontaktní pracoviště umožňují optimální dostupnost nabízených služeb. Evidovaných certifikátu je na statisíce.

---

[26] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. s. 122 ISBN 80-7263-125-X.

[27] *Kvalifikovaná certifikační autorita* [online]. 2011 [cit. 2011-03-17]. Dostupný z WWW: <http://www.cpost.cz/cz/sluzby/e-sluzby/kvalifikovana-certifikacni-autorita-id287/>.

I. CA vydává kvalifikované certifikáty určené zejména pro komunikaci v oblasti orgánů veřejné moci. Výjimkou není ani Okresní soud v Ostravě, pro který I. CA vydala kvalifikovaný certifikát, na jehož základě je využíván elektronický podpis.[28]

2.5 Časové razítko

Časové razítko je podobně jako certifikát elektronický dokument. Kvalifikovaným časovým razítkem je datová zpráva, kterou vydává kvalifikovaný poskytovatel certifikačních služeb a jež důvěryhodným způsobem spojuje data v elektronické formě s časovým okamžikem. Kvalifikované časové razítko je schopno zaručit, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.[29]

Kvalifikované časové razítko, které určuje zákon č. 440/2004 Sb. musí obsahovat:

- určení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal,
- číslo kvalifikovaného časového razítka jedinečné u daného kvalifikovaného poskytovatele certifikačních služeb,
- hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka,
- data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno, elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal,
- v případě fyzické osoby jméno, eventuálně jména, příjmení a stát, ve kterém kvalifikovaný poskytovatel sídlí, u právnické osoby obchodní firmu nebo název a stát, ve kterém kvalifikovaný poskytovatel sídlí

[28] *I.CA a.s.* [online]. 2011 [cit. 2011-03-19]. Dostupný z WWW: <http://www.ica.cz/cz/menu/1/obecne-informace/ >.
[29] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace.* 1. vyd. Olomouc: ANAG, 2008. s 149 ISBN 978-80-7263-465-1.

Časovým razítkem se označují datové zprávy v projektu e-Governmentu datové schránky. [30]

Rozdíl mezi certifikátem a časovým razítkem spočívá v tom, že certifikát je vázán na osobu či subjekt majitele, zatímco časové razítko je spojeno s dokumentem.

Časové razítko definuje vlastnosti elektronického dokumentu (čas jeho existence), kdežto certifikát vymezuje vlastnosti subjektu (jeho vazba fyzické a elektronické identity).

Kvalifikované časové razítko má shodné bezpečností atributy jako kvalifikovaný certifikát a lze ho tedy považovat jako dokument stejné důvěryhodnosti.[31]

Ve výše zmíněné kapitole byly vysvětleny základní pojmy, jejichž znalost pomůže čtenáři porozumět obsahu této práce. V následující kapitole bude řešena právní úprava elektronického podpisu, kdy se pozornost zaměří na nejdůležitější právní předpisy spojené s užíváním elektronického podpisu.

[30] *Kvalifikované časové razítko* [online]. 2009 [cit. 2011-03-20]. Dostupný z WWW: <http://www.aipsafe.cz/cs/datove-schranky/pojmy/kvalifikovane-casove-razitko/>.
[31] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 149 ISBN 978-80-7263-465-1.

3. Právní úprava elektronického podpisu

V této části diplomové práce se čtenář seznámí s právní úpravou elektronického podpisu, především je zde detailně rozebrán zákon o elektronickém podpisu. Rovněž je věnována pozornost nařízení vlády, kterým se provádí zákon o elektronickém podpisu; vyhlášce o elektronických podatelnách a vyhlášce o postupech kvalifikovaných poskytovatelů certifikačních služeb. Zmíněn je zde rovněž občanský zákoník. Závěrem této kapitoly je komentována směrnice Evropského parlamentu a Rady o zásadách společenství pro elektronické podpisy. Znalost výše zmíněných právních předpisů je nezbytná pro správné užívání elektronického podpisu na Okresním soudě v Ostravě, což jen podtrhuje důležitost této kapitoly.

3.1 Zákon č. 227/2000 Sb., o elektronickém podpisu

V České republice je zásadním legislativním dokumentem z pohledu elektronického podpisu zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.[32]

Česká republika přijala tento zákon v roce 2000 a stala se tak třetí zemí, kde vstoupil v platnost zákon upravující užívání elektronického podpisu. Zákon byl dále novelizován, naposledy zákonem č. 281/2009 Sb. a zákonem č. 424/2010 Sb.[33]

V současné době zásadní roli kontrolního a akreditačního orgánu v duchu zákona zastává Ministerstvo vnitra ČR. V rámci svých povinností ministerstvo dohlíží na dodržování zákona o elektronickém podpisu, uděluje akreditaci poskytovatelům certifikačních služeb a vyhodnocuje shody nástrojů elektronického podpisu s požadavky stanovenými zákonem.[34]

[32] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 111 ISBN 978-80-7263-465-1.
[33] *Zákon č. 227/2000 Sb., o elektronickém podpisu* [online]. 2010 [cit. 2011-03-21]. Dostupný z WWW: <http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx/ >.

Zákon upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb, kontrolu povinností vymezených tímto zákonem a sankce za nedodržení povinností stanovených tímto zákonem.[35]

Význam zákona o elektronickém podpisu spočívá v možnosti použití digitálního podpisu v rámci elektronické komunikace jako náhrady podpisu vlastnoručního při běžné listinné formě komunikace. Zákon vznikl na základě směrnice Evropské unie 1999/93/EC ze dne 13. 12. 1999.[36]

Existence zákona o elektronickém podpisu umožnila přípravu některých základních předpisů pro aplikaci tohoto zákona v oblasti veřejné správy. Z tohoto důvodu bylo v návaznosti na zákon o elektronickém podpisu přijato nařízení vlády č. 304/2001 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

Jeho náplní je právní úprava základních organizačně technických opatření orgánů veřejné moci včetně územních samosprávných celků, jenž provádí výkon státní správy v rámci přenesené působnosti. Na základě těchto opatření je zabezpečena povinnost výše zmíněných orgánů přijmout podání učiněné v elektronické podobě, které bude podepsané elektronicky. Toto nařízení zároveň stanoví pro orgány veřejné moci povinnost zřídit pro příjem a odesílání datových zpráv pracoviště splňující požadavky na technické a programové vybavení a umožňující užívání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.[37]

Novela zákona o elektronickém podpisu (č. 440/2004 Sb.) nabyla účinnosti dne 26. 7. 2004. Toto ustanovení nově zavádí pojmy kvalifikované časové razítko (prokazuje existenci elektronického dokumentu v čase) a elektronické značky.

---

[35] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 111 ISBN 978-80-7263-465-1.

[36] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. s. 122 ISBN 80-7263-125-X.

[37] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. s. 10-11 ISBN 80-7263-125-X.

Dne 15. 4. 2010 nabyla platnost novela zákona o elektronickém podpisu (č. 101/2010 Sb.). Tento předpis v reakci na rozhodnutí 2009/767/ES přidává Ministerstvu vnitra povinnost vést a zveřejňovat seznam důvěryhodných certifikačních služeb. Dále stanoví orgánům veřejné moci povinnost akceptovat kvalifikované certifikáty vydané v ostatních členských státech EU.[38]

3.1.1 Vymezení pojmů dle zákona o elektronickém podpisu

Elektronický podpis - V zákoně č. 227/2000 Sb., o elektronickém podpisu, se pod tímto pojetím rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a umožňují ověření totožnosti podepsané osoby. Datová zpráva je tedy podepsána, v případě že je opatřena elektronickým podpisem.

Jestliže se neprokáže opak, předpokládá se, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.

Datová zpráva – elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, užívaných při zpracování a přenosu dat elektronickou formou. Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Použití zaručeného elektronického podpisu zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána, toto porušení bude možno zjistit.

Podepisující osoba – fyzická osoba, která je držitelem nástroje pro vytváření elektronických podpisů; jedná svým jménem případně jménem jiné fyzické či právnické osoby.

[38] *Zákon č. 227/2000 Sb., o elektronickém podpisu* [online]. 2010 [cit. 2011-03-21]. Dostupný z WWW: <http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx/ >.

3.1.2 Povinnosti podepisující osoby

Mezi povinnosti podepisující osoby patří:

- zacházet s prostředky i daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití
- okamžitě uvědomit poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát o tom, že hrozí nebezpečí zneužití dat pro vytváření zaručeného elektronického podpisu
- podávat pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu

3.1.3 Povinnosti poskytovatele certifikačních služeb

Poskytovatel certifikačních služeb, jenž vydává kvalifikované certifikáty je povinen:

- zajistit, aby certifikáty jím vydané obsahovaly všechny náležitosti kvalifikovaných certifikátů
- zajistit, aby údaje v certifikátech byly přesné, úplné a pravdivé
- zajistit, aby se každý mohl ujistit o identitě poskytovatele certifikačních sužeb a jeho kvalifikovaném certifikátu
- zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů a údaje v něm obsažené při každé změně aktualizovat
- používat bezpečné systémy a nástroje elektronického podpisu a zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují
- zajistit, aby datum a čas kdy je kvalifikovaný certifikát vydán nebo zneplatněn, mohly být přesně určeny a tyto údaje byly dostupné třetím stranám
- mít k dispozici finanční zdroje na provoz v souladu s požadavky v zákoně uvedenými a s ohledem na riziko odpovědnosti za škody

- uchovávat veškeré dokumenty a informace o vydaných kvalifikovaných certifikátech po dobu deseti let od ukončení platnosti kvalifikovaného certifikátu; dokumenty a informace může uchovávat v elektronické podobě

Poskytovatel certifikačních služeb, jenž vydává kvalifikované certifikáty, vydává podepisujícím osobám kvalifikované certifikáty na základě smlouvy, ta musí být písemná.

Poskytovatel současně nesmí uchovávat a kopírovat data pro vytváření zaručeného elektronického podpisu osob, kterým poskytuje své certifikační služby. Je nezbytné, aby poskytovatel certifikačních služeb ukončil platnost certifikátu, pokud podepisující osoba o to požádá, eventuálně v případě, že byl certifikát vydán na základě chybných či nepravdivých údajů.[39]

3.2 Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu

Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů schválila vláda dne 25. srpna 2004.

Toto nařízení vlády stanoví povinnost orgánů veřejné moci zřídit ePodatelny nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím ePodatelny jiného úřadu. Další povinnosti spočívají ve vybavení příslušných zaměstnanců, kteří jsou oprávněni činit právní úkony v oblasti orgánů veřejně moci, kvalifikovanými certifikáty vydanými akreditovanými poskytovateli certifikačních služeb a zajištění ochrany zpracovávaných informací odpovídajícím způsobem.

Orgán veřejné moci na své úřední desce zveřejní informace potřebné k doručování datových zpráv orgánu veřejné moci. Mezi tyto informace patří např. elektronická adresa elektronické podatelny, kontaktní údaje pro přijímání datových zpráv na technických nosičích, zásady potvrzování doručení datových zpráv apod. [40]

[39] *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů*
[40] *Nařízení vlády č.495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu*

3.3 Vyhláška č. 496/2004 Sb., o elektronických podatelnách

Vyhláška upravuje postupy, jak mají orgány veřejné moci přijímat a odesílat datové zprávy prostřednictvím elektronické podatelny a strukturu údajů kvalifikovaného certifikátu, na základě kterých lze podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat.

Tato vyhláška navazuje na nařízení vlády č.495/2004 Sb. k elektronickým podatelnám, které nařizuje orgánům veřejné moci zřídit elektronickou podatelnu a má sloužit jako návod, jak naplnit podmínky dané tímto nařízením vlády. [41]

3.4 Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb

V první části vyhlášky, která je určena poskytovatelům certifikačních služeb, jsou obsaženy požadavky na jejich postupy při vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. Druhá část se vztahuje na označující osoby, především na orgány veřejné moci. Zabývá se požadavky na ochranu soukromých klíčů, které jsou použity při vytváření elektronických značek.[42]

3.5 Zákon č. 40/1964 Sb., občanský zákoník

V § 40 tohoto zákona je upraveno samotné použití elektronického podpisu v obecné rovině. Tento paragraf uvádí, že písemný právní předpis je platný v případě, že je podepsán jednající osobou; jestliže činí právní úkon více osob, nemusí být jejich podpisy na stejné listině. V případech, kdy je to obvyklé, může být podpis nahrazen mechanickými prostředky. Jestliže je právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů. Zachovává se písemná forma v případě, že právní úkon je učiněn dálnopisem, telegraficky či elektronickými prostředky, které umožňují zachytit obsah právního úkonu a určit osobu, která právní úkon učinila.

[41] Vyhláška č. 496/2004 Sb., o elektronických podatelnách

[42] *Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb* [online]. 2010 [cit. 2011-03-23]. Dostupný z WWW:<http://www.mvcr.cz/clanek/vyhlaska-c-378-2006-sb-o-postupech-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb.aspx

Z výše uvedeného tedy vyplývá, že došlo ke zrovnoprávnění dokumentů a podpisů, prováděných klasicky v listinné podobě a podpisů elektronických. Je však nezbytné, aby se smluvní strany na použití elektronického podpisu dohodly.[43]

3.6 Směrnice 1999/93/EC Evropského parlamentu a Rady, o zásadách společenství pro elektronické podpisy

Cílem této směrnice je umožnit využití elektronických podpisů a přispět k jejich právnímu uznávání. Tato směrnice stanovuje právní rámec pro elektronické podpisy a některé certifikační služby, aby bylo možné zajistit řádné fungování vnitřního trhu.

Směrnice očekává využití elektronického podpisu jako nástroje k ověřování dat elektronickou cestou v mnoha oblastech lidské činnosti, ať už mezi orgány státní správy a samosprávy navzájem či jejich komunikaci s občany např. v oblasti sociálního zabezpečení, veřejných zakázek, daní, zdravotnictví či soudnictví. Nezbytnou podmínkou pro takové využití je plná právní uznatelnost elektronického podpisu a jeho přípustnost jako důkazu v soudním řízení.

Směrnice se nevztahuje na hlediska spojená s uzavíráním a platností smluv či jiných právních závazků. Směrnicí nejsou také dotčena pravidla a omezení, která upravují používání dokumentů a která jsou obsažena v právních předpisech Společenství nebo ve vnitrostátních právních předpisech. Na základě směrnice Evropské unie 1999/93/EC vznikl v České republice zákon o elektronickém podpisu, což jen dokládá důležitost této směrnice.

Jedním z podstatných přínosů Směrnice je zavedení společné terminologie ve vztahu k elektronickému podpisu. Ta se následně přenáší do lokálních legislativ, což zvyšuje srozumitelnost pojmů. Směrnici lze považovat za podrobný dokument zabývající se nejen definicí, ale také tvorbou a ověřením vlastního elektronického podpisu, právní uznatelnosti v zemích EU, způsoby akreditace, procesy vydávání certifikátů a dalšími službami poskytovatelů certifikačních služeb.[44]

[43] *Zákon č. 40/1964 Sb., občanský zákoník*
[44] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. s. 44-49 ISBN 80-7263-125-X

Směrnici Evropského parlamentu a Rady 1999/93/ES je možné hodnotit jako klíčový dokument pro rozvoj elektronického podpisu v Evropě. Je však na místě uvést podstatnou nevýhodu Směrnice. Tou je její benevolence v oblastech, které by měly být striktně definovány. Namísto termínů „musí“ a „nesmí“ se využívají termíny „měl by“ či „neměl by“.

Tento výklad vede ke skutečnosti, že dochází k velké vůli ve výkladu Směrnice pro její následnou aplikaci v lokálních legislativách, což směruje k omezené kompatibilitě a ztěžuje nejen přenositelnost technologií mezi státy EU, ale také zpomaluje výměnu dat a mezinárodní obchod.[45]

V této kapitole se čtenář seznámil s právní úpravou elektronického podpisu. Zmíněny byly všechny podstatné právní předpisy, jejichž znalost je nezbytná pro správné užívání elektronického podpisu. V následující kapitole je zaměřena pozornost na využití elektronického podpisu v praxi.

[45] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 109 ISBN 978-80-7263-465-1.

4. Využití elektronického podpisu v praxi

V této části práce jsou řešena následující témata: využití ePodatelny soudy; Pravidla pro zajištění provozu ePodatelny na Okresním soudě v Ostravě; Postup Okresního soudu v Ostravě při komunikaci prostřednictvím datové schránky a je zde také vysvětleno vydávání certifikátů od společnosti Česká pošta, s. p. Neopomenul jsem také přiblížit potenciální problémy, které jsou s elektronickým podpisem spojené.

V rámci této kapitoly je provedena analýza využití elektronického podpisu na Okresním soudě v Ostravě prostřednictvím dotazníkového šetření. Předmětem analýzy je aplikovaný výzkum exploračního typu formou dotazníkového zkoumání zaměřeného na využití elektronického podpisu v organizaci veřejné správy. Objektem šetření jsou zaměstnanci Okresního soudu v Ostravě.

Pro Okresní soud sídlící v Ostravě-Porubě je využití elektronického podpisu samozřejmostí. S nárůstem moderních výpočetních technologií vzrostl požadavek na kvalitní počítačovou techniku, rychlejší připojení k internetu, k ochraně počítačů a celých sítí před viry a dalšími ilegálními aktivitami, s čímž jsou spojeny vyšší náklady na provoz těchto sítí a pracovišť.

Elektronický podpis na Okresním soudě v Ostravě se využívá od srpna roku 2009. Dle Pravidel pro zajištění provozu elektronické podatelny na Okresním soudě v Ostravě, je elektronická podatelna opatřena zaručeným elektronickým podpisem za organizaci. Kvalifikovaný certifikát vydala První certifikační autorita, a.s.

Každý zaměstnanec Okresního soudu v Ostravě vypravující poštu má svůj elektronický podpis, který může však používat pouze k pracovním účelům. Úředníci soudu využívají pro komunikaci prostřednictvím datových schránek elektronický podpis s certifikátem České pošty, s. p. (PostSignum CA).

4.1 Využití ePodatelny soudy

Od října 2007 byl spuštěn provoz první složky projektu elektronizace justice: ePodatelna. Ta fakticky zavádí na soudy institut přijímání elektronických podání se zaručeným (uznávaným) elektronickým podpisem bez nutnosti dalšího doplňování podání, což má za cíl zrychlit a zlevnit soudní řízení. Podoba ePodatelny je zobrazena na obrázku 4.1

Projekt ePodatelna, jenž je v provozu pro soudy je tedy výchozím programem celého projektu eJustice. Elektronický spis zajistí do budoucna možnost propojení informačních systémů v justici a skutečné převedení soudních spisů do elektronické podoby.

V případě, že se občan chce obrátit na soud ať už z důvodu podání žaloby, hromadného či jiného podání je pro něj vhodné využít ePodatelnu. V případě chybějících údajů ePodatelna občana okamžitě upozorní a ten se tak vyhne situaci, kdy mu soud podání několikrát vrátí k doplnění kvůli formálním nedostatkům.

Projekt ePodatelna nejen urychlí a zlevní administrativní procesy, ale zároveň usnadní práci profesionálům a veřejnosti. Elektronická podatelna je určena pro uživatele disponující zaručeným kvalifikovaným elektronickým podpisem.[46]

Elektronická podatelna přijímá podání od subjektů prostřednictvím internetu (mail, web) a distribuuje je organizacím resortu. Současně dohlíží nad správností elektronických podpisů podání a zajišťuje bezpečnost přenosů.[47]

Od 1. 1. 2008 je možné s využitím zaručeného elektronického podpisu komunikovat se soudem v rámci agendy insolvenčního práva. Od 1. 7. 2008 lze zaslat soudům návrh na vydání elektronického platebního rozkazu opatřeného zaručeným elektronickým podpisem.[48]

---

[46] *ePodatelna* [online]. 2008 [cit. 2011-03-28]. Dostupný z WWW: <http://obcanskyzakonik.justice.cz /ejustice/epodatelna.html/ >.
[47] Uživatelská příručka ePodatelny [online]. 2010 [cit. 2011-03-28]. Dostupný z WWW: <http://epodatelna .justice.cz/ePodatelna/epo1200new/form.do/ >.
[48] STAŇKOVÁ, M. Počty nevyřízených věcí se snižují. *Zpravodajský měsíčník pro státní správu a podnikatele* [online]. 2008 [cit. 2011-03-28]. Dostupný z WWW: <http://www.parlament-vlada.cz/modules.php?name=News&file=print&sid=504/>.

Státní instituce včetně soudů, ale také soukromé firmy různých typů užívají při své práci **datové schránky**. Využívání datových schránek konkrétně na soudech výrazně urychluje soudní jednání, jednání soudů s ostatními státními institucemi a úřady. Komunikace mezi zmíněnými úřady často vázla právě na nevyzvednuté poště.

Je výrazně simplifikován proces doručování písemností, které jsou v elektronické podobě mnohem jednodušeji zasílány. Datovou schránku musí mít odesílatel i příjemce. Právem a povinností všech uživatelů datových schránek je pravidelně kontrolovat a přebírat poštu.

Datové schránky jsou využívány od listopadu roku 2009. Za dobu čtyř měsíců užívání jimi prošlo více než dva miliony zpráv. Jak uvádí report Ministerstva spravedlnosti, justice se na celkovém počtu odeslaných a přijatých zpráv podílí zhruba 40 procenty.

Konkrétní čísla hovoří o celkem 6 316 126 zpráv, z toho 2 362 142 zpráv bylo adresováno či odešlo z adresy patřící některému z orgánů resortu justice. Ze schránek orgánů justice odešlo 1 510 301 datových zpráv.

Nejaktivnější byl přitom Okresní soud Ostrava, jehož zprávu našlo ve své schránce 67 982 adresátů. Ve schránkách úřadů, které spadají pod resort justice, se pak objevilo 851 841 zpráv. I zde na čele pomyslného žebříčku figuruje ostravský okresní soud, který přijal 40 124 zpráv.

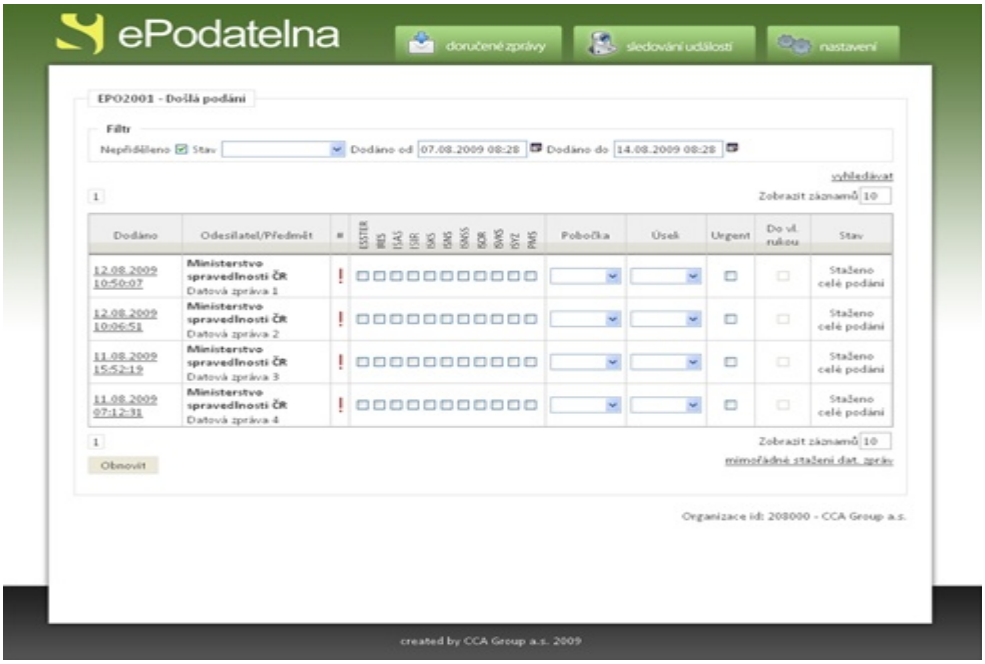
Zprovoznění systému využívání datových schránek s sebou přineslo i řadu problémů jak organizačního, tak technického rázu. Z tohoto důvodu byl vypracován materiál na zmírnění těchto chyb. Ministerstvo spravedlnosti na odstranění vad intenzivně pracuje.

Cílem je, aby systém pomáhal a plnil svou funkci co nejefektivněji, než aby komplikoval a zpomaloval celý soudní systém.[49]

[49] ŽIŽLAVSKÁ, V. Datové schránky – justice. *Mediafax* [online]. 2010 [cit. 2011-03-28]. Dostupný z WWW: <http://www.mediafax.cz/domaci/3004277-Datovymi-schrankami-ktere-vyuziva-ceska-justice-jiz-prosly-vice-nez-dva-miliony-zprav/>.

Procesní předpisy myslí i na situaci, kdy dojde k výpadku provozu datových schránek. Dle občanského soudního řádu jestliže není možné doručit dokument prostřednictvím veřejné datové sítě do datové schránky, soud ji doručí prostřednictvím doručujícího orgánu, účastníkem řízení či jeho zástupcem. Náhradní postup doručení je řešen také v trestním řádu (§ 62 tr.ř.) a v soudním řádu správním (§ 42 s. ř. s.).[50]

Obrázek 4.1 ePodatelna



Zdroj: *Internetové stránky CCA Group.* Dostupný z WWW: <http://www.cca.cz >. [citováno 2011-03-22].

4.2 Pravidla pro zajištění provozu ePodatelny na Okresním soudě v Ostravě

Z výše zmíněného reportu Ministerstva spravedlnosti je patrné jak důležitou roli představuje pro Okresní soud v Ostravě využívání datových schránek. Jestliže má být docíleno bezproblémového chodu elektronické podatelny je nezbytné stanovit pravidla, kterými se bude soud řídit.

[50] *Změny v systému doručování v resortu justice* [online]. 2009 [cit. 2011-03-29]. Dostupný z WWW: <http://portal.justice.cz/Justice2/MS/ms.aspx?j=33&o=23&k=5208&d=308460/ >.

Poslední úprava pravidel pro zajištění provozu elektronické podatelny byla zkompletována na Okresním soudě v Ostravě dne 22. 10. 2010. Pravidla jsou stanoveny dle zákona č. 227/2000 Sb. v platném znění; vyhlášky č. 496/2004 Sb.; nařízení vlády č. 495/2004 Sb. v souladu s Instrukcí MSp č. 13/2002-OI-SP.

Elektronickou podatelnou určenou pro příjem a odesílání datových zpráv je na Okresním soudě v Ostravě elektronická adresa: podatelna@osoud.ova.justice.cz.

Elektronická podatelna přijímá pouze datové zprávy ve formátech: doc – Word 2000, excel 2000, rtf, txt a pdf.

Nejvyšší přípustná velikost přijímané e-mailové zprávy včetně přílohy je 1,5 MB. Souhrnný denní limit pro přijetí datových zpráv s elektronickým podpisem je z technicko-administrativních důvodů nastaven na velikost 10 MB.

Datové zprávy na technickém nosiči dat (CD-R+/- nebo DVD-R+/-) jsou přijímány na sekretariátu předsedy soudu, přičemž je nezbytné, aby byly ve výše zmíněných formátech. Datová zpráva v jiném formátu ani spustitelné soubory (např. .COM, .EXE apod.) nebude přijata. Jestliže je možné z přijaté datové zprávy zjistit elektronickou adresu odesílatele, bude odesílateli zasláno sdělení o nesplnění podmínek k přijetí datové zprávy.

V případě, že datová zpráva je doručena na elektronickou podatelnu v souladu s požadovanými formáty, dochází k neprodlenému potvrzení doručení. Odesílateli se zašle datová zpráva, pokud je z přijaté datové zprávy možno zjistit elektronickou adresu odesílatele. Zpráva se nešifruje a je elektronicky podepsána uznávaným elektronickým podpisem Okresního soudu v Ostravě na základě kvalifikovaného certifikátu.

Zpráva o potvrzení doručení bude vždy obsahovat:

- datum a čas doručení datové zprávy s uvedením hodiny, minuty a sekundy [51]
- charakteristiku datové zprávy umožňující její identifikaci
- elektronický podpis za organizaci

[51] Jedná se o datum a čas, kdy je datová zpráva fyzicky uložena do databáze Okresního soudu v Ostravě. Nejedná se o datum, kdy byla datová zpráva zaslána podatelem z jeho počítače. Tento datum a čas je stěžejní vzhledem k začátku řešení procesu (od této doby jsou k dispozici zaměstnancům organizace, dříve nikoliv). Zapsaná podání musí mít ověřený elektronický podpis.

Pokud potvrzení doručení datové zprávy nedojde, zpráva nebyla doručena. Vzor zprávy o potvrzení doručení:Vaše datová zpráva týkající se ……..…. byla elektronické podatelně Okresního soudu v Ostravě doručena dne …… v …hod. …min. …sek.

Doručená datová zpráva je prověřena pracovnicí soudu a následně předána příslušnému oddělení soudu. Jestliže se u datové zprávy zjistí škodlivý kód, není zpracována. Pokud z přijaté datové zprávy lze určit elektronickou adresu odesílatele, je na tuto adresu zasláno sdělení o nalezení škodlivého kódu.

Je na místě také zmínit, že mohou nastat další situace, na základě kterých je nutné odeslat zprávu podateli o neověření podpisu. Jedná se o tyto případy:

- *Certifikát není od české akreditované CA* – k podání je připojen elektronický podpis založený na certifikátu, jenž nebyl vydán českou akreditovanou certifikační autoritou dle zákona č. 227/2000 Sb. o elektronickém podpisu. Z tohoto důvodu bude elektronický certifikát posuzován z hlediska akreditace certifikační autority v Evropském společenství.

  Pokud bude připojený elektronický podpis vydán akreditovanou certifikační autoritou z Evropského společenství, je potřeba, aby o této skutečnosti podatel informoval Okresní soud v Ostravě do tří dnů od přijetí podání organizací. Pokud elektronický podpis nebude vydán akreditovanou certifikační autoritou, bude na podání nahlíženo jako na nepodepsané podání.

- *Certifikát byl neplatný již před doručením podání do ePodatelny* - připojený uznávaný elektronický podpis je založený na certifikátu, kterému skončila platnost před doručením podání na Okresní soud v Ostravě, a proto na podání bude nahlíženo jako na nepodepsané podání.

- *Certifikát byl před odesláním zprávy zneplatněn* - připojený uznávaný elektronický podpis k uvedenému podání je neplatný, jelikož jeho certifikát byl před doručením podání zneplatněn.

- *Podpis nebo certifikát vykazuje nějakou chybu* - připojený elektronický podpis nebo jeho certifikát obsahuje chybu, a proto na podání bude nahlíženo jako na nepodepsané podání. Jedná se např. o situaci, kdy je zpráva po podepsání změněna.

Všechny přijaté a odeslané datové zprávy se ukládají na vyhrazené místo v počítačové síti. Ukládaní a archivace počítačových údajů se řídí Instrukcí MSp č. 75/99-OI.

Soud přijímá prostřednictvím elektronické podatelny především podání učiněná dle zákona č. 99/1963 Sb. – občanského soudního řádu a dle zákona č. 141/1961 Sb. – trestního řádu.

Elektronická podatelna je opatřena zaručeným elektronickým podpisem za organizaci. Kvalifikovaný certifikát vydala První certifikační autorita a.s. pod sériovým číslem 10514800.[52]

4.3 Postup Okresního soudu v Ostravě při komunikaci prostřednictvím datové schránky

Postupy pro komunikaci s veřejnými datovými schránkami jsou stanoveny především ve vyhlášce č. 37/1992 Sb. o jednacím řádu pro okresní a krajské soudy, ve znění pozdějších předpisů.

Instrukce MSp č. j. 505/2001 – Org, vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy, ve znění pozdějších předpisů stanoví *postup při odesílání písemností prostřednictvím datové schránky:*

1. Písemnost, která je určena účastníkovi řízení se vypracuje v příslušném informačním systému soudu. Originál se následně vytiskne, podepíše a založí do spisu. Elektronická podoba (např. elektronický stejnopis rozhodnutí) se uloží v tomto systému.

2. V informačním systému se zjistí, zda osoba vlastní datovou schránku. Jestliže ano, doručuje se elektronický stejnopis rozhodnutí nebo jiná písemnost v elektronické podobě prostřednictvím datové schránky. V případě, že osoba nemá datovou schránku, stejnopis rozhodnutí nebo jiné písemnosti v listinné podobě se zasílají prostřednictvím doručujícího orgánu (např. soudním doručovatelem, držitelem poštovní licence).

[52] GOTWALDOVÁ, D. Pravidla pro zajištění provozu ePodatelny. *Justice* [online]. 2010 [cit. 2011-03-29]. Dostupný z WWW:<http://portal.justice.cz/Justice2/Soud/soud.aspx?o=157&j=167&k=1610&d=191378/>.

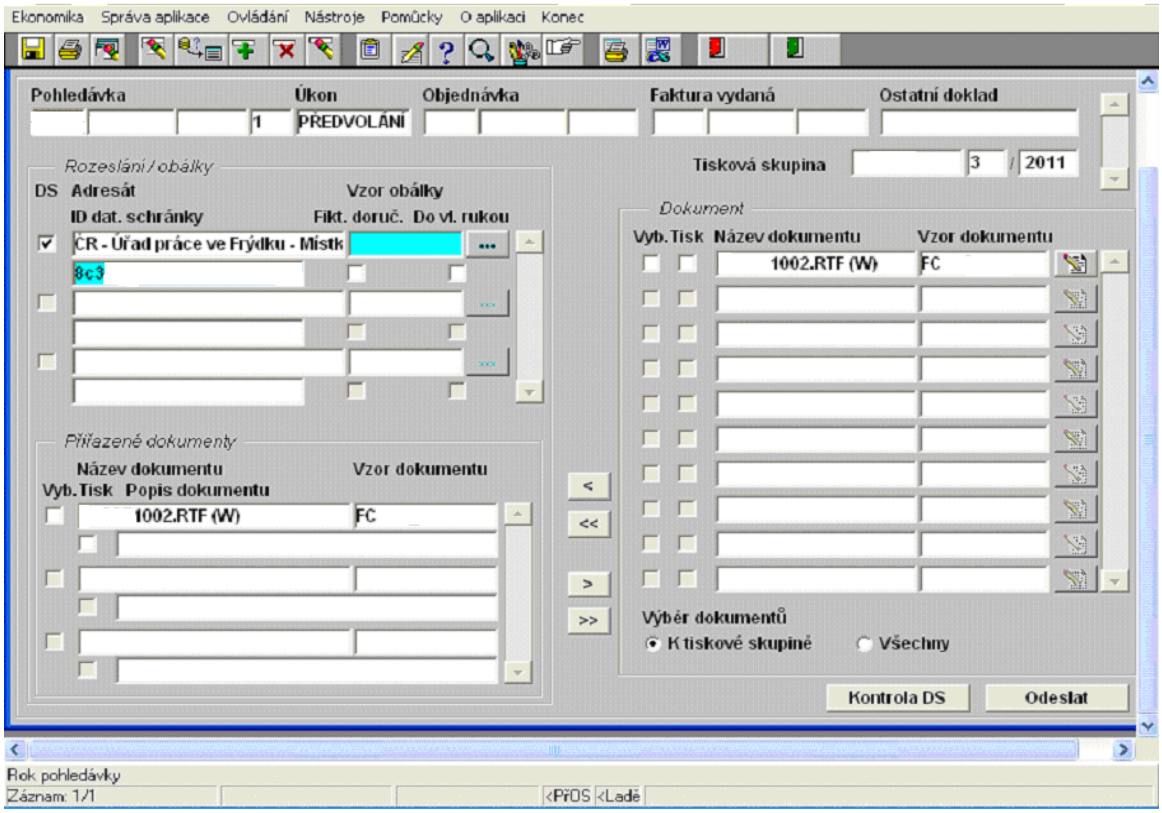
V následujícím příkladě zaměstnanec soudu učiní dotaz na vybranou instituci prostřednictvím datové schránky. Nežli tak učiní, musí si vybrat adresáta, kterého chce prostřednictvím datové schránky kontaktovat.

Zaměstnanci Okresního soudu v Ostravě nejčastěji podepisují dokumenty v rámci datových schránek zaručeným zaměstnaneckým podpisem při následujících dotazech:

- Dotaz na úřad práce
- Dotaz na okresní správu sociálního zabezpečení
- Dotaz – šetření v evidenci vězňů (v rámci celé ČR)
- Dotaz na věznici (konkrétní věznici)
- Dotaz na zdravotní pojišťovnu
- Dotaz na zaměstnavatele
- Dotaz na magistrát – odbor dopravy
- Dotaz na ukončení likvidace
- Dotaz na peněžní ústav
- Dotaz na finanční úřad

V našem případě, si zaměstnanec soudu vybral Úřad práce ve Frýdku – Místku, odbor kanceláře úřadu – oddělení exekucí a součinnosti. Po výběru adresáta přiřadí ID datové schránky adresáta a připojí dokument k odeslání. Tuto situaci znázorňuje obrázek 4.2, uvedený na následující straně.

Obrázek 4.2 Komunikace prostřednictvím datové schránky

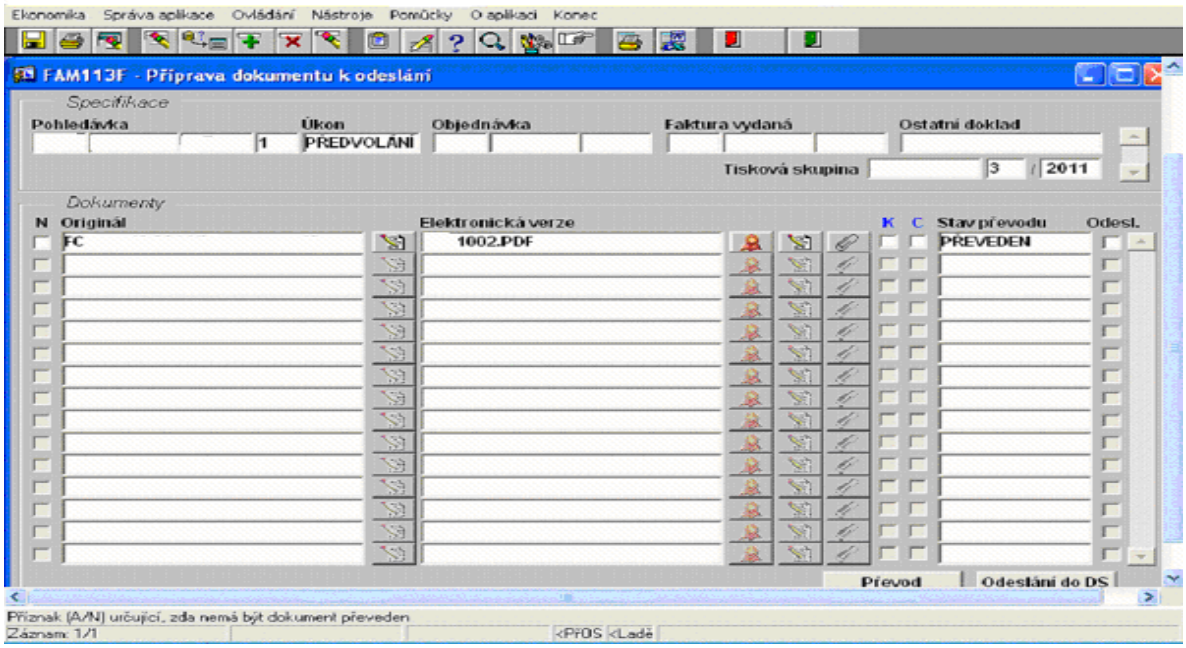


Zdroj: *Interní dokumenty*

3. V následujícím kroku se písemnost převede do formátu PDF (funkcí v příslušném informačním systému). Do formátu PDF nejsou převáděny vzory k vyplnění a také písemnosti, které jiný účastník zaslal na soud písemně a které byly naskenovány.

Jak lze vidět na obrázku 4.3 na další straně, původní přiřazený dokument s označením 1002.RTF (W) se převedl do elektronické verze: 1002.PDF. Tato situace je patrná u „stavu převodu“, kde je uvedeno: PŘEVEDEN.

Obrázek 4.3 Příprava dokumentu k odeslání

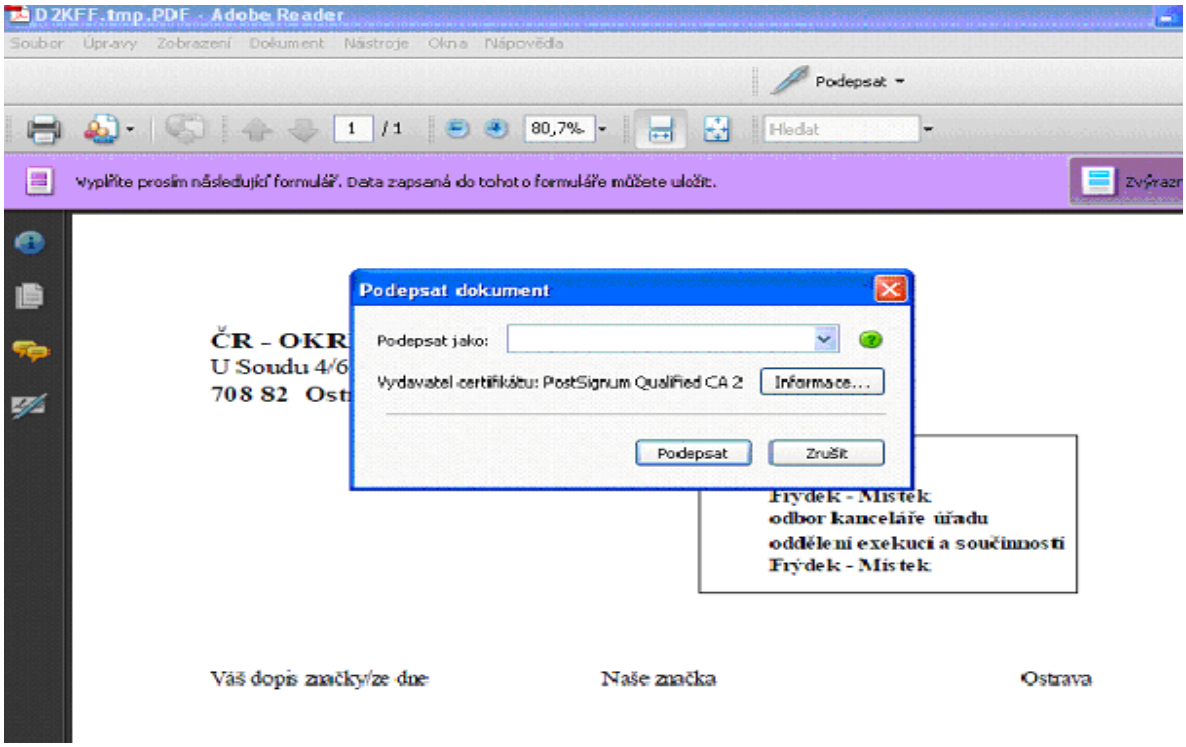


Zdroj: *interní dokumenty*

4. Jestliže je písemnost převedena do PDF je nutné provést kontrolu, zda převod proběhl úspěšně.

5. Převedená písemnost do PDF se podepíše zaručeným zaměstnaneckým podpisem.

Obrázek 4.4 Podepsání dokumentu zaručeným zaměstnaneckým podpisem



Zdroj: *interní dokumenty*

Ve výše zmíněném obrázku 4.4 u textu „podepsat jako“ zaměstnanec soudu uvede své jméno a dokument podepíše. U položky „informace“ obsažené v tabulce jsou uvedeny informace o elektronickém podpisu, jakými jsou:

- platnost elektronické podpisu (1 rok)
- vydavatel : PostSignum Qualified CA 2, Česká pošta, s.p.
- zamyšlené použití: transakce podepisování; podepisování dokumentu, šifrování klíče
- veřejný klíč: RSA
- důvěryhodnost

Jakmile zaměstnanec dokument podepíše, uloží změny a ověří informace, zda elektronický podpis je platný, nezměnil se a je podepsán současným uživatelem. Zároveň ověří, zda podpis je označen časovým razítkem.

6. Takto podepsaná písemnost je zaslána do eVýpravny.[53]

Stav doručení písemnosti je evidován informačním systémem soudu. Údaj o stavu doručení písemností se vytiskne a založí do příslušného spisu, který nahrazuje současnou doručenku.

Existují dokumenty, které nelze zaslat do datové schránky. Jedná se o písemnosti:

- obsahující utajované informace
- jejichž povaha zasílání do datové schránky neumožňuje (kolek, směnka atd.)
- odlišné dokumenty, u nichž je dle zákona stanoven jiný způsob doručování

[53] eVýpravna zajišťuje spolehlivé vypravení dokumentů v elektronické podobě do datové schránky nebo na jinou elektronickou adresu

Postup při přijímání písemností doručovaných do datové schránky soudu:

1) Každé zaslané podání se vytiskne.

2) Ověří se platnost elektronického časového razítka.

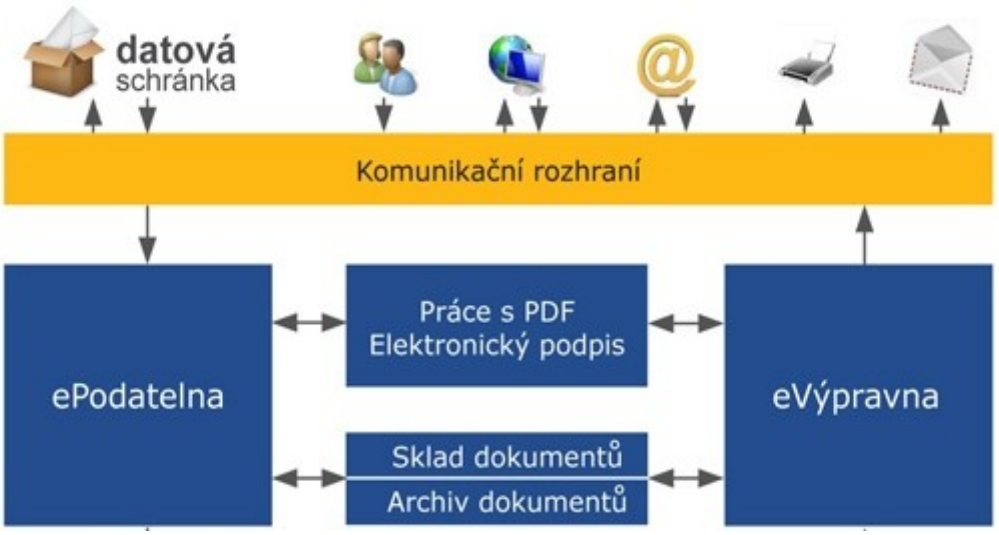
3) Jestliže se jedná o písemnost k určité spisové značce, tato písemnost je předána příslušné kanceláři. Jedná-li se o nové podání, provede se zápis do příslušného rejstříku.

4) Každé podání se zároveň ukládá do příslušného informačního systému.

5) Konverze se provádí výhradně na pokyn soudce (Vyššího soudního úředníka, asistenta, apod.)[54]

Celkový průběh komunikace prostřednictvím datové schránky lze vidět na obrázku 4.5.

Obrázek 4.5 Celkový průběh komunikace prostřednictvím datové schránky



Zdroj: *Internetové stránky CCA Group.* Dostupný z WWW: <http://www.cca.cz >. [citováno 2011-03-27].

[54] SMEJKAL, V. Datové schránky nastupují. *IHNED* [online]. 2009 [cit. 2011-04-01]. Dostupný z WWW: <http://pravniradce.ihned.cz/c1-37865170-datove-schranky-nastupuji/>.

4.4 Vydávání certifikátů od společnosti Česká pošta, s.p. žadatelům

Nežli je žadateli (v našem případě zaměstnanci Okresního soudu v Ostravě) vydán certifikát musí si na svém počítači vygenerovat klíčový pár a elektronickou žádost o certifikát. Z tohoto důvodu jsou na webových stránkách CA k dispozici příslušné nástroje.

Žadatel navštíví pracoviště České pošty se službou Czech POINT osobně. Nelze zplnomocnit svého zástupce či provést dálkové vydání certifikátu. Na tuto pobočku, kde se vydávají a zneplatňují certifikáty, si s sebou donese občanský průkaz nebo pas k ověření totožnosti společně s vygenerovanou žádostí o certifikát (na USB flash paměti či ID žádosti uložené na webovém serveru). Zaměstnanec České pošty ověří identitu žadatele a zkopíruje osobní doklad totožnosti žadatele, což je stanoveno v zákoně o elektronickém podpisu. Následně se vytiskne písemná žádost o certifikát, kterou žadatel svým podpisem schválí. Žádost obsahuje heslo pro zneplatnění. Z důvodu bezpečnosti je vhodné, aby se heslo neshodovalo s jinými hesly, které žadatel běžně užívá.

Vydaný certifikát lze přijmout potvrzením přijetí přes webové stránky PostSignum na základě došlého mailu či osobně podepsáním protokolu o vydání certifikátu. Certifikát je v tomto případě uložen na přenosné médium zákazníka.

Žadatel má právo vydaný certifikát odmítnout. Pokud by jej odmítl, vytiskne se protokol o nevydání certifikátu a certifikát se zneplatní. Jestliže žadatel má zájem o nový certifikát musí si nejprve vygenerovat nový klíčový pár a žádost o certifikát, s kterými navštíví pobočku České pošty znovu.

Certifikát se instaluje do aplikace, ve které byly vygenerovány klíče. Jestliže tato aplikace je určena pouze pro generování klíčů, provádí se export do souboru a následně dochází k natažení do cílové aplikace. Společně s vydaným certifikátem je nutné nainstalovat do cílové aplikace rovněž certifikáty certifikačních autorit PostSignum CA. Jestliže dojde k situaci, kdy již nelze užívat klíče a vystavený certifikát (např. z důvodu havárie či odcizení počítače), je nutné požádat o zneplatnění certifikátu, jenž koresponduje se ztraceným (prozrazeným) soukromým klíčem.

Certifikát je platný jeden rok. Poté je potřeba zažádat o nový certifikát. V případě, že nedojde ke změně osobních údajů zaměstnance nebo údajů v certifikátu, je možné následný certifikát vystavit: pomocí webové aplikace, osobní návštěvou pobočky České pošty se službou Czech POINT či prostřednictvím elektronicky podepsaného e-mailu odeslaného na podatelnu postsignum. Informace o možnosti obnovy certifikátu jsou rovněž uvedeny v e-mailové zprávě, jež je odeslána před koncem platnosti certifikátu.

V případě, že nastaly změny, je potřeba doručit na pobočku České pošty se službou Czech POINT změnu údajů pro vydání certifikátu. Provedou se příslušné změny v systému CA a poté se zaměstnanec může dostavit na pobočku pošty nechat si vydat nový certifikát. Obnova certifikátu je zpoplatněna.

Smlouva se obvykle uzavírá na dobu neurčitou. Na jednu smlouvu lze vydat libovolné množství certifikátů. Dle ceníku České pošty, jenž je platný od 1. 4. 2011 je cena kvalifikovaného certifikátu určeného pro ověření elektronického podpisu zaměstnance 396 Kč. Jelikož Okresní soud v Ostravě potřebuje pro výkon svých zaměstnanců velký počet zaměstnaneckých elektronických podpisů opatřených kvalifikovaným certifikátem, rád jistě využije slevu za množstevní odběr certifikátů, kterou Česká pošta nabízí.

Nárok na množstevní slevu spočívá v odebrání minimálního počtu 50 certifikátu v období od 1. 1. 2011 do 31. 12. 2011. Sleva se navyšuje v závislosti na počtu odebraných kusů.[55]

4.5 Problémy spojené s elektronickým podpisem

Aplikace elektronického podpisu v praxi s sebou přináší překážky, které se ve světě papírových dokumentů nevyskytují, případně jsou již vyřešeny. Jeden z největších problémů, který doposud nebyl vyřešen v oblasti elektronicky zpracovávaných a předávaných dokumentů, je **archivace**.

Zatímco archivace papírových dokumentů je dennodenní rutina mnoha úřadů a firem, v elektronické oblasti je situace odlišná. Mezi klíčové požadavky na archivaci elektronických dokumentů patří: průkaznost, čitelnost a dostupnost.

---

[55] *Internetové stránky Certifikační autority PostSignum.* Dostupný z WWW: < http://www.postsignum.cz >. [citováno 2011-03-24].

Právě zajištění dostupnosti elektronických dokumentů je nejsnáze řešitelným požadavkem, neboť jsou k dispozici technologie, které zajistí dostatečnou dostupnost strukturovaných dat či nestrukturovaných dokumentů.

Řada obchodních a legislativních procesů požaduje, aby dokumenty, které jsou součástí těchto procesů, byly dostupné minimálně po dobu 10 let. Zatímco v oblasti papírových dokumentů se nejedná o neřešitelný problém, v elektronickém světě je tato doba téměř nepředstavitelně dlouhá. Vývoj technologií pro výměnu dat totiž přináší časté změny. Právě relativně častá změna standardů v oblasti datových formátů je hlavním problémem v čitelnosti a zobrazitelnosti archivovaných dat po delší době archivace.

Z pohledu archivace elektronických dokumentů jsou jednoznačně nejvhodnější jednodušší, dobře popsané formáty, které nepodléhají častým změnám a nejsou svázány s jednou technologií či výrobcem. Takovýmto formátem pro textové dokumenty může být prostý textový formát (txt) či formát pdf, který byl přijat také jako standard ISO. V případě, že je požadováno, aby elektronický podpis byl opatřen zaručeným elektronickým podpisem, musí použitý formát podporovat příslušnou technologii.

V současné době lze za nejvhodnější řešení pro dlouhodobou archivaci považovat metodu migrace, která je založena na transformaci dat z jednoho formátu do druhého, aktuálního. Nejvhodnější postup začíná výběrem vhodného datového formátu. Jestliže vybraný formát již nevyhovuje kritériu prezentovatelnosti obsahu, je na základě migračních schémat připravena transformace (migrace) do nového formátu. Ačkoliv se zdá tento postup ideální, má své chyby. Jednou z nich je ztráta integrity dat při migraci, což představuje významnou chybu při archivaci elektronicky podepsaných dokumentů, jelikož je porušen elektronický podpis a bezpečností atributy dokumentu.

Východisko z této situace lze nalézt prostřednictvím užití důvěryhodné instituce. Ta migraci provede s tím, že sice dojde k porušení původních bezpečnostních mechanismů dokumentu, ale při migraci vzniknou nové, které vytvoří důvěryhodná a nezpochybnitelná instituce. Tato instituce tedy ověří původní bezpečnostní atributy dokumentu a vydá o tom potvrzení, které přidá k migrovanému dokumentu.[56]

[56] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 144 -146 ISBN 978-80-7263-465-1

Také samotný elektronický podpis „vyprchává“, jelikož jeho důvěryhodnost časem klesá z důvodu poklesu bezpečnosti užitých kryptografických algoritmů. Řešením tohoto problému je opakované využití technologie časových razítek.

Mezi další problém spojený s elektronickým podpisem patří **průkaznost provedené operace.** Zatímco v oblasti papírových dokumentů lze provedení závažných úkonů doložit, např. klient při zaplacení poplatku na přepážce získá příjmový doklad, v elektronickém světě je to komplikovanější. Ačkoliv zákon o elektronickém podpisu dává nástroj, prostřednictvím kterého lze doložit, že daný dokument má příslušná osoba k dispozici (elektronický podpis) a že existoval v daném čase (časové razítko), nelze využít nějakého nástroje, který by mohl prokázat, že s tímto dokumentem byla provedena nějaká operace.

Zvláštním bodem v rámci prokazování provedených operací je prokazování odeslání a předání dat. Zákon o e-Governmentu doručení a potvrzení řeší. Očekává se, že celý systém datových schránek bude spravován a provozován důvěryhodnou institucí, která dostatečně doloží prováděné operace spojené s předáváním dokumentů. Dle tohoto zákona však bude systém užíván pouze ke komunikaci jednotlivých subjektů s orgány veřejné moci.

Další komplikace se týká **mezinárodní uznatelnosti elektronického podpisu**. Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy říká, že členské státy mohou požadovat doplňující požadavky u používání elektronických podpisů ve veřejné správě. Tato skutečnost bohužel vede např. k tomu, že český občan ačkoliv podepíše podání uznávaným elektronickým podpisem v souladu s českou legislativou a s daty spojenými s kvalifikovaným certifikátem vydaným v České republice, nebude uznáno za podepsané a důvěryhodné. Obdobně problematická je také situaci v oblasti poskytování certifikačních služeb. Jelikož mezinárodní uznávání elektronického podpisu lze považovat za jeden z nejzávažnějších problémů, jenž omezuje širší uplatnění této technologie v praxi, je nezbytné najít vhodné řešení. Východiskem by byla obecně uznávaná a zároveň závazná pravidla, která by sjednocovala požadavky na elektronický podpis minimálně v zemích EU.[57]

[57] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. s. 146 -147 ISBN 978-80-7263-465-1.

4.6 Analýza využití elektronického podpisu na Okresním soudě v Ostravě

V níže uvedených kapitolách se budu zabývat nejpodstatnější části diplomové práce a to vymezením předmětu analýzy, postupy a metodami analýzy, výsledky šetření a jejich interpretací v přehledných grafech, shrnutím nejpodstatnějších skutečností a následně návrhy a doporučeními pro zkvalitnění využití elektronického podpisu.

4.6.1 Vymezení předmětu analýzy

Cílem aplikovaného výzkumu, který jsem provedl v rámci této diplomové práce, bylo zhodnotit úroveň využití elektronického podpisu na Okresním soudě v Ostravě. Předmětem je aplikovaný výzkum exploračního typu formou dotazníkového zkoumání zaměřeného na využití elektronického podpisu v organizaci veřejné správy. Objektem šetření jsou zaměstnanci Okresního soudu v Ostravě.

Význam dotazníkového šetření spočívá v nalezení odpovědí na předem vybrané otázky, ze kterých se následně pokusím vypracovat návrhy a doporučení pro zkvalitnění využití elektronického podpisu na Okresním soudě v Ostravě.[58]

4.6.2 Postup a metody analýzy

Pro získání informací nezbytných pro vypracování této diplomové práce včetně získání odpovědí na předem vybrané otázky jsem využil následující metody:

- rozhovor
- studium dostupných dokumentů
- anonymní dotazníkové šetření

[58] REICHEL, J. *Kapitoly metodologie sociálních výzkumů*. 1. vyd. Praha: Grada Publishing, 2009. s. 33 - 34 ISBN 978-80-247-3006-6.

Rozhovor

V rámci vysokoškolského bakalářského studia jsem vykonával praxi na Okresním soudě v Ostravě, což zvýšilo mé podvědomí nejen o této instituci, ale zároveň o jejím chodu. V té době se o elektronickém podpisu na soudě hodně hovořilo, neboť od srpna roku 2009 měl začít být využíván.

Prostřednictvím rozhovorů, které jsem nyní se zaměstnanci popisované organizace vedl, jsem zjistil důležité skutečnosti, které jsem následně využil při vypracování této diplomové práce.

Studium dostupných dokumentů

V rámci studia dostupných dokumentů jsem se seznámil s dokumenty, které souvisejí s fungováním elektronického podpisu na Okresním soudě v Ostravě. Jedná se např. o Pravidla pro zajištění provozu ePodatelny či Postupy při komunikaci prostřednictvím datových schránek. Materiály jsem prostudoval a posléze z nich vybral nejdůležitější informace.

Dotazník

Dotazník jakožto jednu z technik sociologického výzkumu jsem využil k získání podstatných informací pro naplnění cíle diplomové práce, tedy zhodnocení využití elektronického podpisu na Okresním soudě v Ostravě.

Dotazník je souhrn písemně zaměřených otázek, jejichž odpovědi poskytují údaje o názorech v určité skupině osob. Jelikož je dotazník chápán jako levný, nenáročný způsob pro kvantitativní výzkum, využívá se často jako forma analýzy.

Část otázek v dotazníku jsou formulovány tak, aby respondent mohl uvést své názory ohledně elektronického podpisu. Zbývající otázky jsou uzavřené s možností výběru z připravených odpovědí. Údaje respondentů byly zpracovány anonymně. Vyhotovený dotazník je součástí přílohy č. 1. Účelem dotazníku je získané informace zanalyzovat a zformovat do přehledných grafů s vysvětlením.[59]

[59] REICHEL, J. *Kapitoly metodologie sociálních výzkumů*. 1. vyd. Praha: Grada Publishing, 2009. s. 110 – 118 ISBN 978-80-247-3006-6.

4.6.3 Výsledky analýzy a jejich interpretace

Jelikož není možné oslovit všechny objekty šetření ze základního souboru, vzniká výběrový soubor. V rámci dotazníkového zkoumání jsem se dotazoval 70 respondentů, z nichž mi 51 dotazník vyplnilo.

Nejvyšší návratnosti dotazníků jsem dosáhl prostřednictvím osobního dotazování, kdy z 35 dotazovaných mi dotazník vyplnilo 33. Co se týče elektronického dotazování, které jsem rovněž využil, již návratnost nebyla tak velká. Z 35 zaslaných dotazníků mi přišlo 18 vyplněných. Z těchto výsledků je patrné, že osobní dotazování má u respondentů větší šanci na úspěch respektive vyplnění, nežli elektronické dotazovaní, jelikož zaměstnanci mají dostatek své práce a na vyplňování podobných e-mailů nemají čas.

Jakmile jsem získal dostatečný počet vyplněných dotazníků, informace jsem zanalyzoval a převedl do přehledných grafů. V následujícím textu jednotlivé otázky okomentuji dle výsledků z dotazníkového šetření.

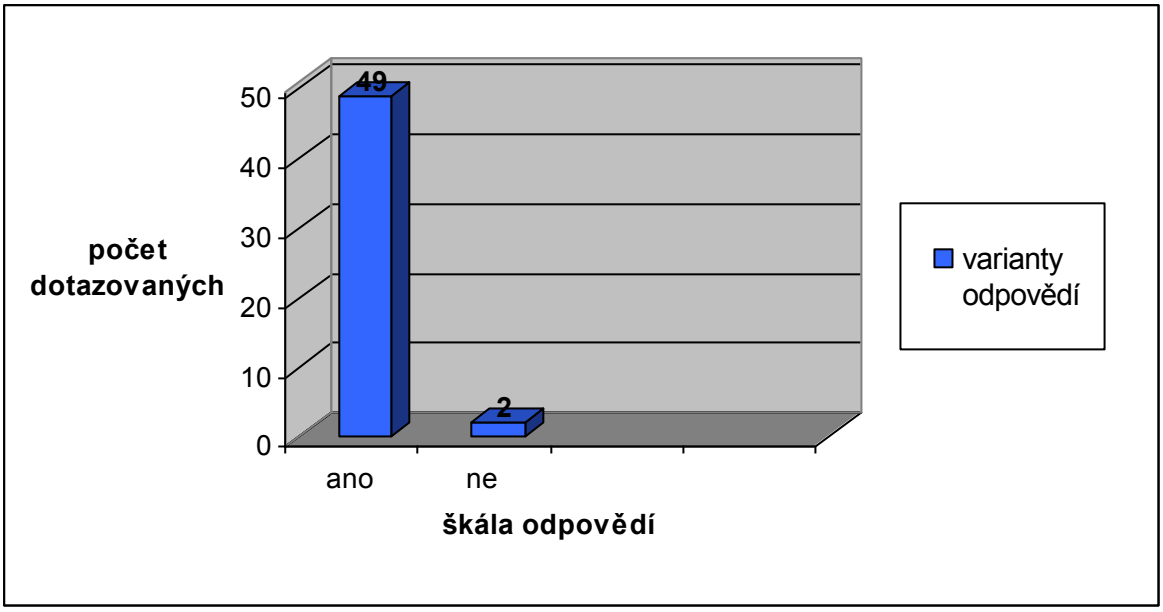
1. U první otázky: **„Víte co je to elektronický podpis?“** měli respondenti na výběr ze dvou odpovědí – ano/ne. Všech 51 respondentů uvedlo odpověď ano. Je tedy zřejmé, že všichni zaměstnanci Okresního soudu v Ostravě ví, co je to elektronický podpis.

Graf 4.6 Znalost elektronického podpisu

Zdroj: *Vlastní zpracování*

2. Druhá otázka s názvem: **„Využíváte elektronický podpis v rámci svého zaměstnání?“** opět dávala dotazovaným na výběr ze dvou odpovědí ano/ne. Pouze 2 zaměstnanci z výběrového souboru uvedli, že elektronický podpis nevyužívají. Tito respondenti poté rovnou přešli na otázku č. 7. Zbývajících 49 zaměstnanců podpis v rámci svého zaměstnání užívají. V rámci svého zaměstnání elektronický podpis nevyužívají soudci, kteří rovněž nevyužívají datové schránky.

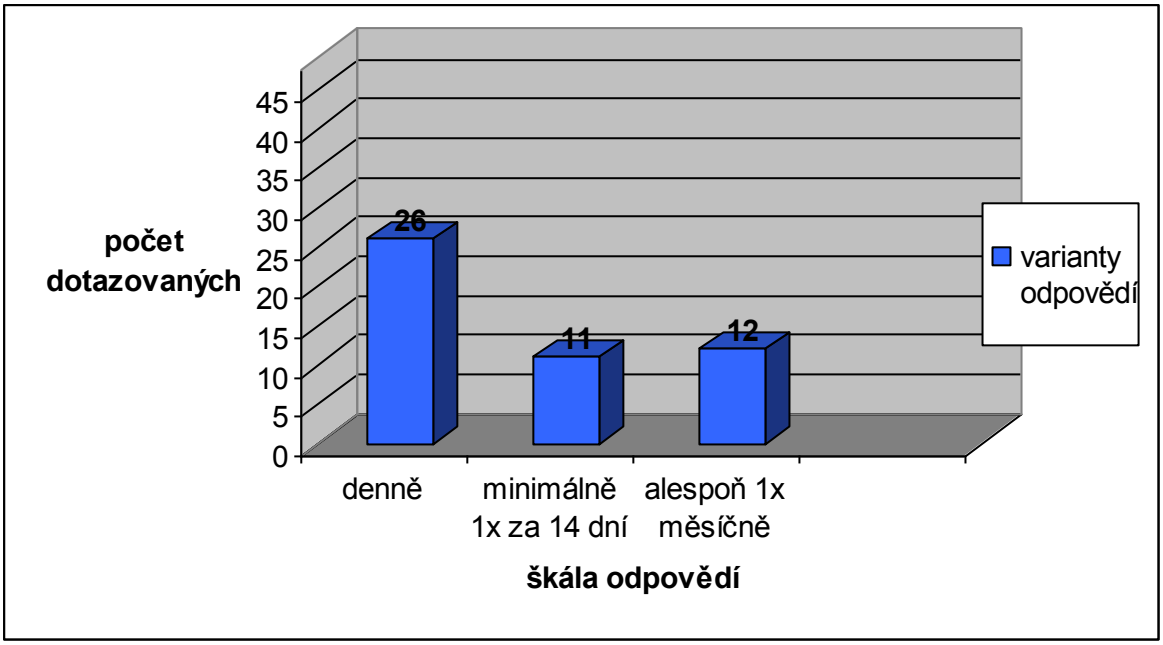
Graf 4.7 Využití elektronického podpisu v zaměstnání



Zdroj: *Vlastní zpracování*

3. Třetí otázka volně navazuje na předchozí dotaz: **„Jak často elektronický podpis využíváte?“** Jelikož dva respondenti elektronický podpis v rámci svého zaměstnání nevyužívají, výběrový soubor se snížil na 49 respondentů. Z tohoto počtu 26 jich využívá elektronický podpis denně, 11 respondentů minimálně 1x za 14 dní a 12 zaměstnanců alespoň 1x měsíčně.

Graf 4.8 Míra využití elektronického podpisu v rámci zaměstnání

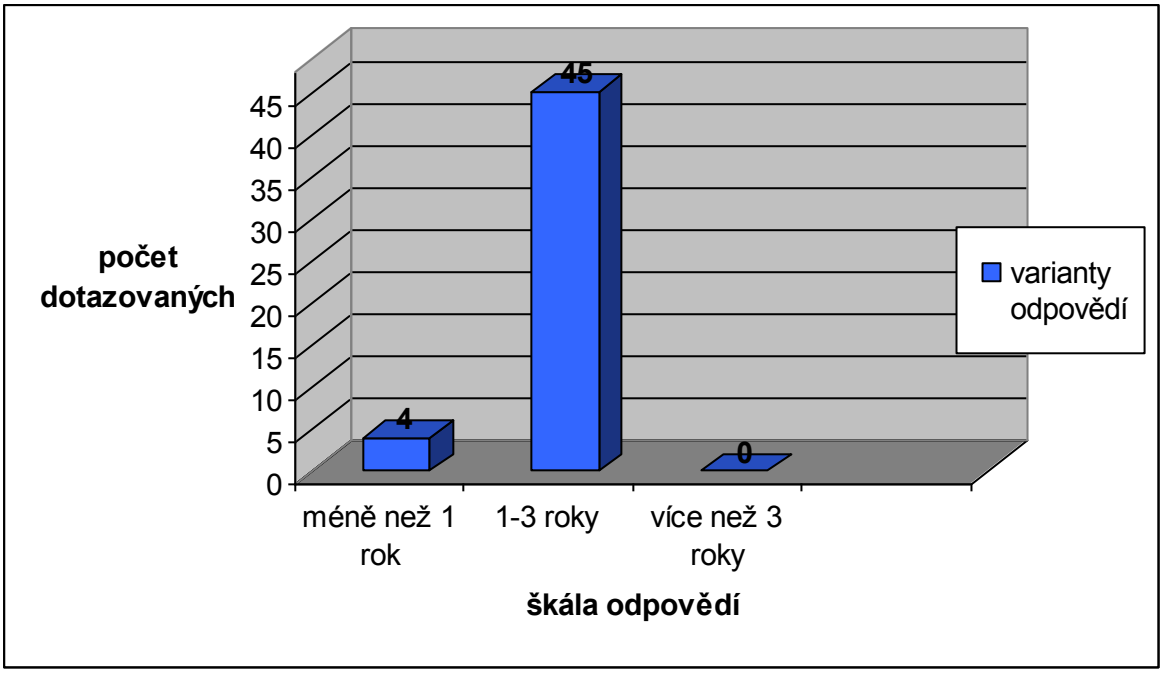


Zdroj: *Vlastní zpracování*

4. Čtvrtá otázka, která patří do kategorie otevřených otázek, zněla: **„Uveďte, při jaké specifické činnosti využíváte elektronický podpis při zaměstnání?“** Odpovědi respondentů zněly: při vyhotovení dokumentů; při zasílání korespondence mezi úřady; po každém vyhotovení dokumentu v PC - před jeho odesláním; při přihlášení do aplikace.

5. Pátá otázka směřovala ke zjištění odpovědi na otázku: **„ Jak dlouho již v rámci své pracovní činnosti elektronický podpis využíváte?“** Z možných variant, 4 dotazovaní uvedli, že méně než 1 rok; 45, tedy drtivá většina uvedla, že využívá elektronický podpis v rozmezí jednoho až tří let. Nikdo z dotazovaných neuvedl, že užívá elektronický podpis více než 3 roky v rámci své pracovní činnosti. Elektronický podpis se na Okresním soudě v Ostravě používá od srpna roku 2009, tuto skutečnost naprostá většina potvrdila v dotazníkovém šetření.

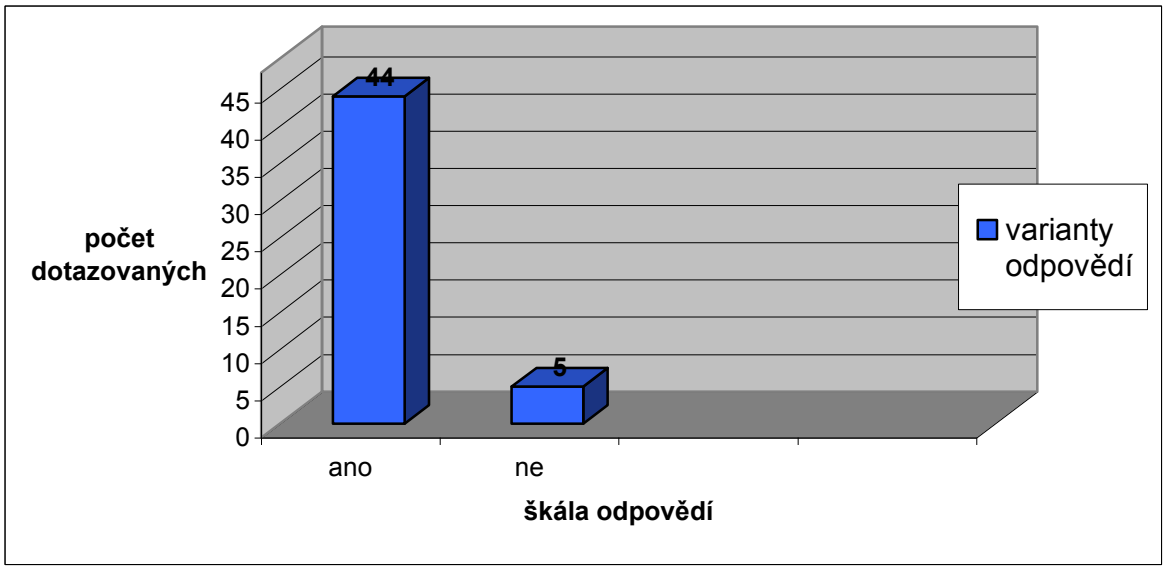
Graf 4.9 Délka využití elektronického podpisu v rámci zaměstnání



Zdroj: *Vlastní zpracování*

6. Otázka s pořadovým číslem šest zněla: **„Byli jste před užíváním elektronického podpisu proškoleni zaměstnavatelem?“** Ze 49 respondentů 44 uvedlo, že ano. Pouze pět uvedlo, že ne. Jejich záporná odpověď může být způsobena tím, že zaměstnanci projdou během své pracovní činnosti řadou školení a následně již nejsou schopni se orientovat, zda dané školení mělo co dočinění s elektronickým podpisem či nikoliv.

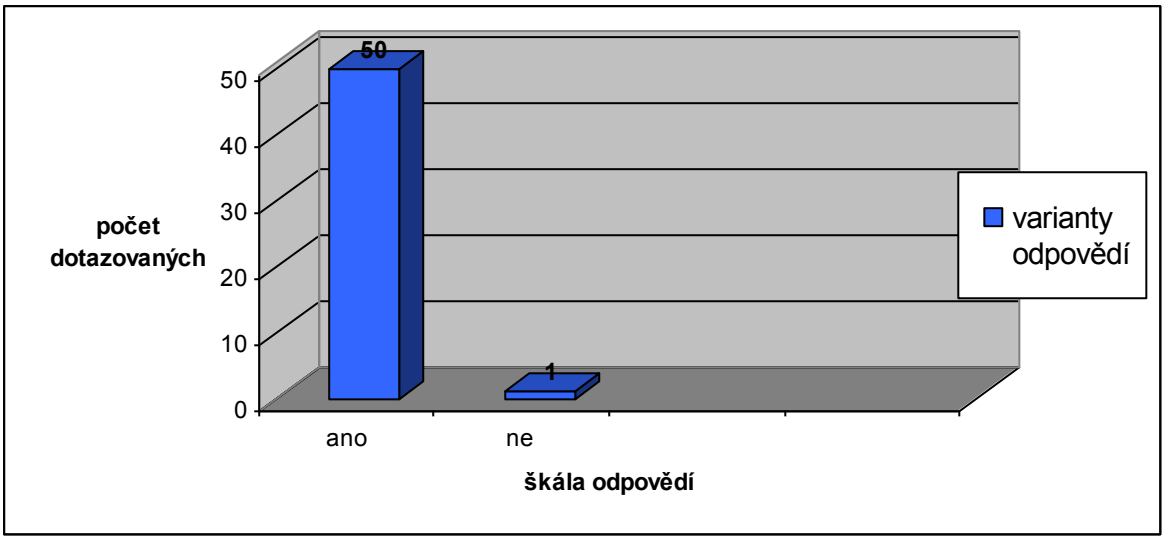
Graf 4.10 Školení zaměstnanců ohledně elektronického podpisu



Zdroj: *Vlastní zpracování*

7. Sedmá otázka: **„Víte, že doba platnosti elektronického podpisu je časově omezena?“** byla položena všem 51 respondentům, neboť na ní mohli odpovídat také osoby, které elektronický podpis nevyužívají v rámci svého zaměstnání. Z dotazníkového šetření vyplynulo, že 50 dotazovaných ví, že doba platnosti elektronického podpisu je časově omezena a pouze jeden respondent uvedl, že neví.

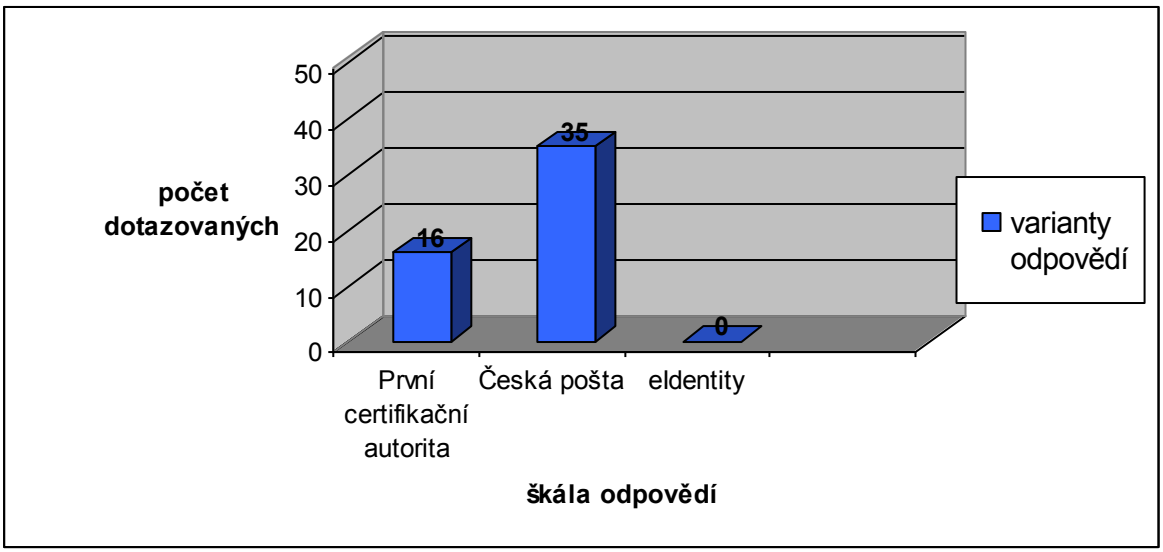
Graf 4.11 Znalost časového omezení platnosti elektronického podpisu



Zdroj: *Vlastní zpracování*

8. Osmou otázku jsem pokládal respondentům v tomto znění: **„Víte, která z uvedených certifikačních autorit poskytuje kvalifikovaný certifikát pro využívání elektronického podpisu na Okresním soudě v Ostravě?“** Jelikož jsou na Okresním soudě v Ostravě využívány dva kvalifikované certifikáty od České pošty, s. p. a První certifikační autority, a.s., byl jsem zvědav, jak respondenti odpoví. Z 51 dotazovaných 12 zatrhlo obě varianty výše zmíněných certifikačních autorit. Celkově tedy z počtu 51 respondentů 16 uvedlo První certifikační autoritu, a.s. a 35 dotazovaných Českou poštu, s. p. Nikdo z dotazovaných nevybral možnost eIdentity, a.s.

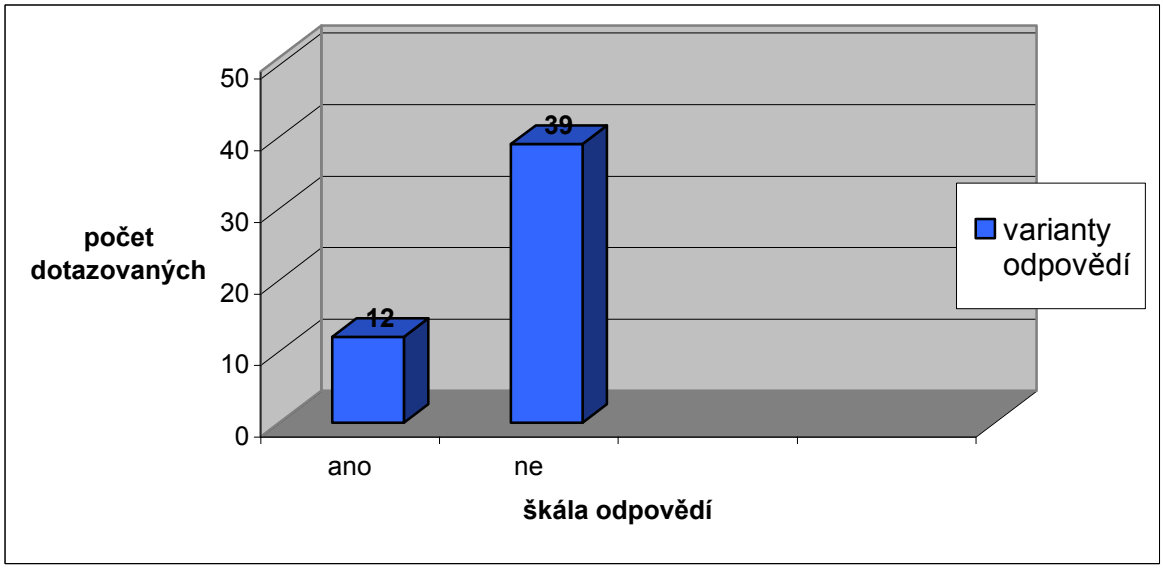
Graf 4.12 Certifikační autority poskytující kvalifikovaný certifikát pro Okresní soud v Ostravě



Zdroj: *Vlastní zpracování*

9. Název deváté otázky zněl: **„Využíváte elektronický podpis v osobním životě?“** Z dotazníkového šetření vyplynulo, že většina dotazovaných (39) elektronický podpis v osobním životě nevyužívá. Pouze 12 respondentů z celkového počtu 51 uvedlo, že elektronický podpis využívá.

Graf 4.13 Využití elektronického podpisu v osobním životě



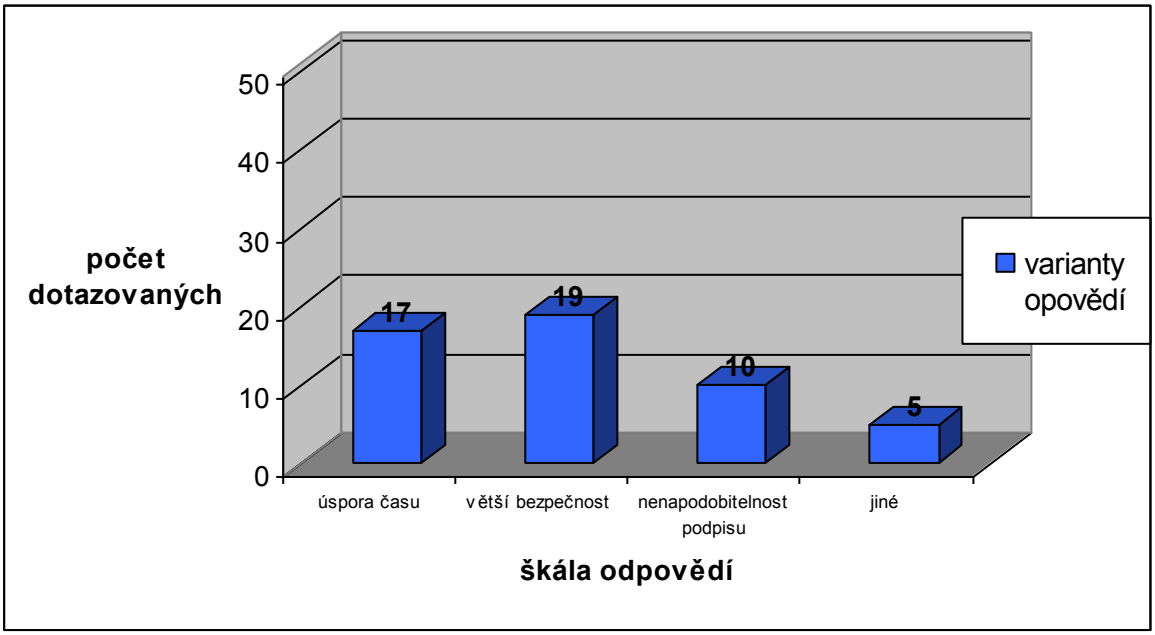
Zdroj: *Vlastní zpracování*

10. Desátá otázka se zaměřila na preference dotazovaných spojených s elektronickým podpisem: **„Jaké výhody spatřujete ve využívání elektronického podpisu?“** U této otázky měli respondenti na výběr ze tří uzavřených možností a jedné otevřené, kde mohli uvést svůj názor na danou problematiku.

Za největší výhodu považují zaměstnanci Okresního soudu v Ostravě větší bezpečnost v rámci elektronické komunikace. Na této variantě se shodlo 19 z celkového počtu 51 respondentů. Následovala úspora času s 17 respondenty a nenapodobitelnost podpisu s 10 dotazovanými.

Možnost napsat vlastní odpověď využilo 5 dotazovaných. V rámci odpovědi uvedli tyto výhody: jednoduché ověření pravosti, neporušenost zprávy, úspora nákladů a nezfalšovatelnost. Poslední odpověď se objevila v dotazníku dvakrát.

Graf 4.14 Výhody ve využívání elektronického podpisu



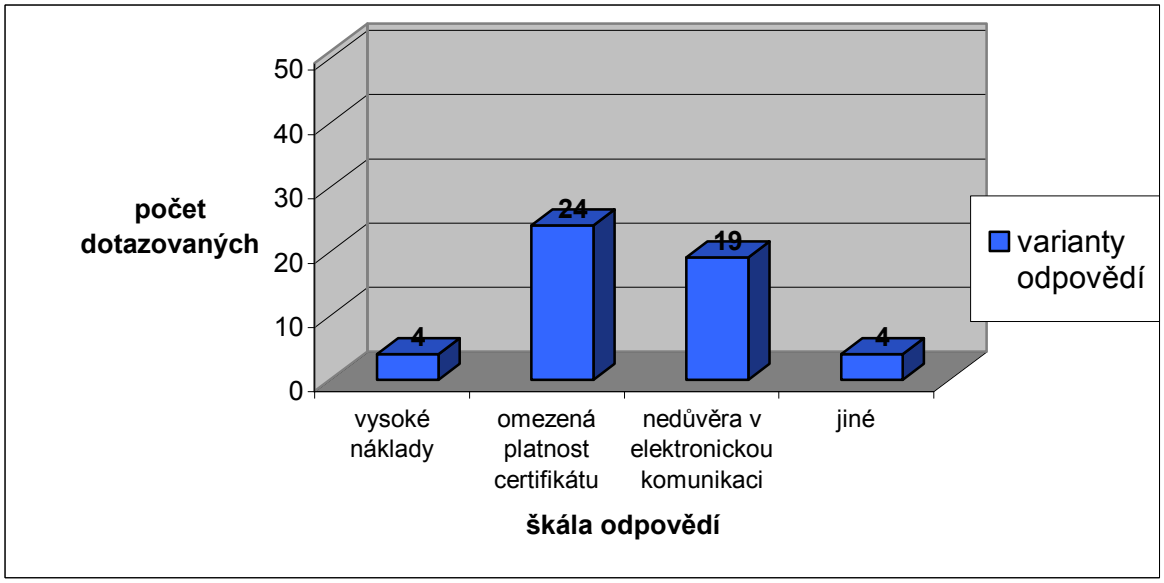
Zdroj: *Vlastní zpracování*

11. Jedenáctá otázka volně navazuje na předchozí otázku: **„Jaké nevýhody spatřujete ve využívání elektronického podpisu?“** U této otázky měli respondenti opět na výběr ze tří uzavřených možností a jedné otevřené, kde mohli uvést svou vlastní odpověď.

Za největší nevýhodu považují respondenti omezenou platnost certifikátu, kdy tuto variantu zvolilo 24 z 51 dotazovaných. Následovala nedůvěra v elektronickou komunikaci s 19 hlasy a vysoké náklady se 4 hlasy.

Pouze 4 osoby využily možnosti uvést svou odpověď. Mezi nevýhody tito dotazovaní uvedli: psychologické bariéry, nízká zodpovědnost lidí vůči svým heslům a problémy s připojením k serveru. Poslední odpověď byla uvedena ve dvou dotaznících.

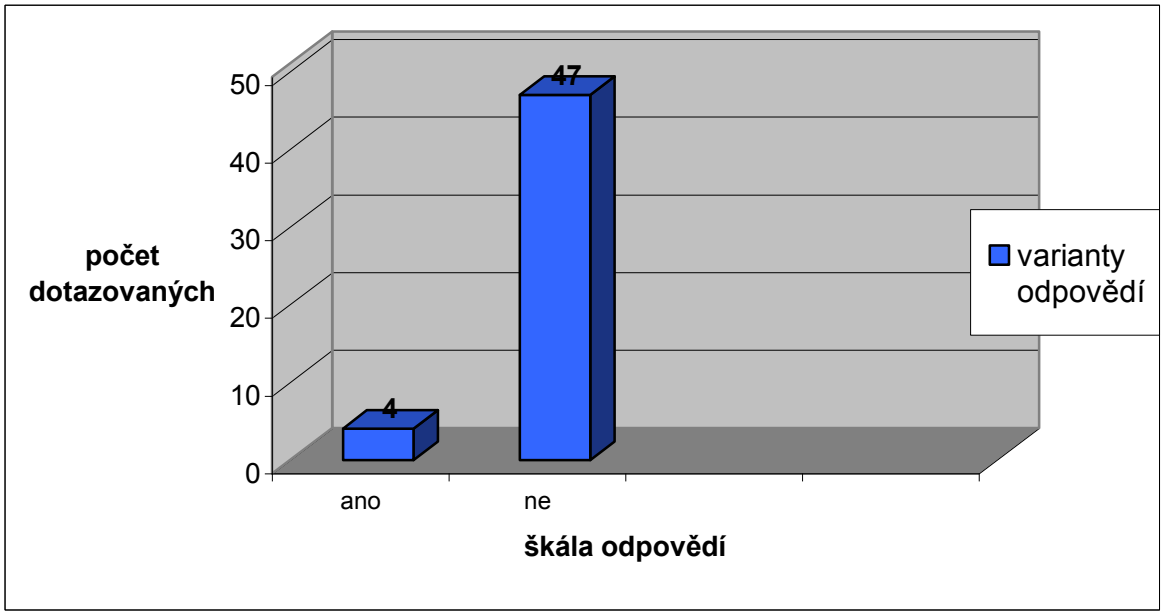
Graf 4.15 Nevýhody ve využívání elektronického podpisu



Zdroj: *Vlastní zpracování*

12. Znění dvanácté otázky: **„Domníváte se, že veřejnost zná elektronický podpis a možnosti jeho využití?"** U této otázky 47 z celkového počtu 51 dotazovaných uvedlo, NE. Pouze 4 osoby se domnívá, že veřejnost zná elektronický podpis a možnosti jeho využití.

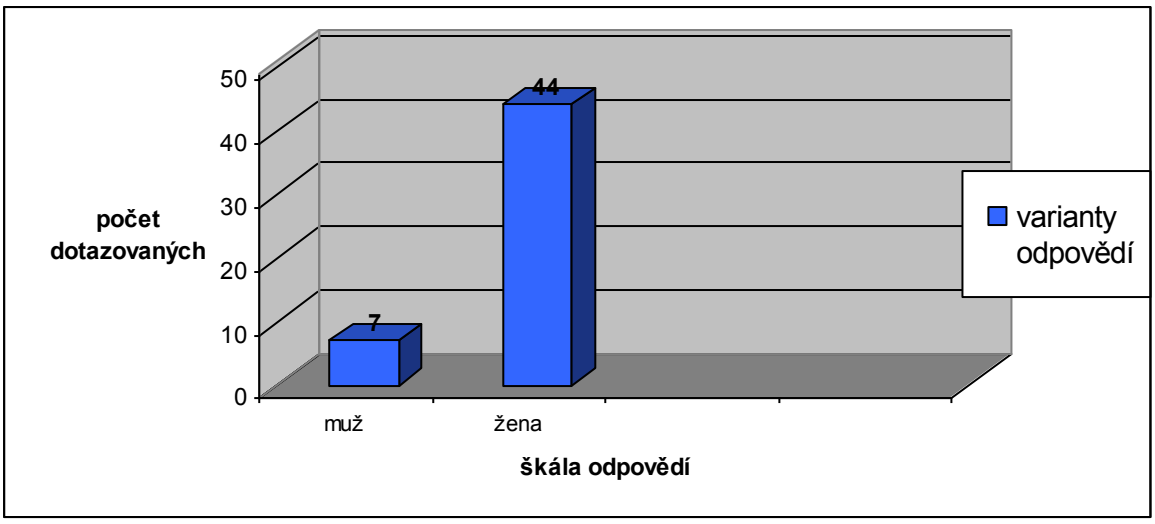
Graf 4.16 Znalost elektronického podpisu a možností jeho využití veřejností



Zdroj: *Vlastní zpracování*

13. Následující dvě otázky se zaměřují na zjištění základních údajů o respondentech. Tou první je tato otázka: **„ Jste muž nebo žena?“** Z dotazníku vyplynulo, že dotazník vyplnily převážně ženy a to v počtu 44 z 51 respondentů. Zbývajících 7 respondentů tvořili muži.

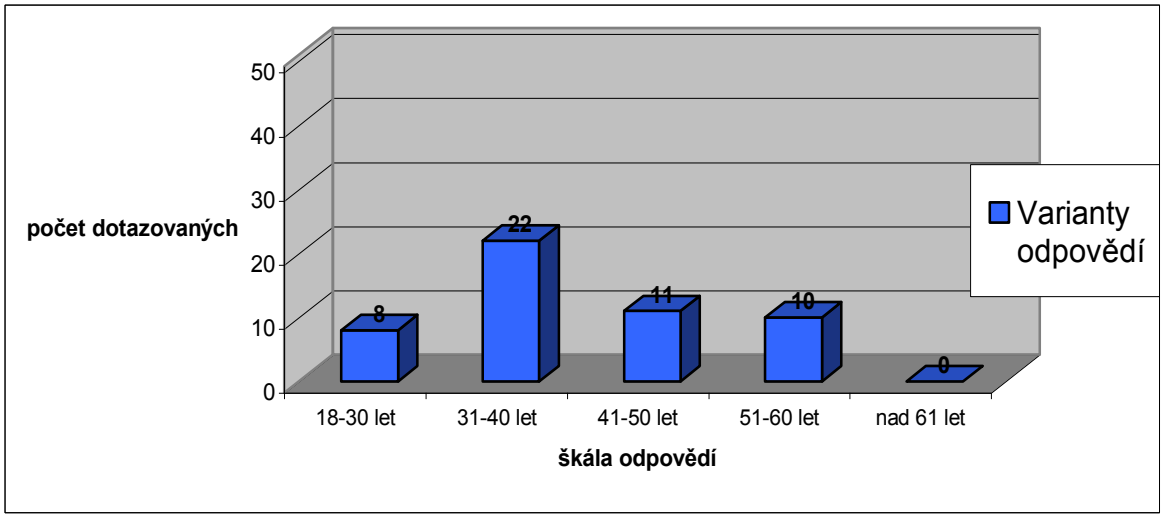
Graf 4.17 Muž či žena



Zdroj: *Vlastní zpracování*

14. Poslední otázka se zaměřuje na věk dotazovaných: **„Kolik je Vám let?“** Z vyplněných dotazníků mi vyšly následující údaje: největší zastoupení z respondentů měli zaměstnanci ve věku 31-40 let a to ve 22 případech, následovali zaměstnanci ve věku 41-50 let a to v 11 případech, ve věku 51-60 let vyplnilo dotazník 10 osob, u věkové kategorie 18-30 let to bylo 8 osob, žádný z respondentů ve věku nad 61 let mi dotazník nevyplnil.

Graf 4.18 Věk respondentů



Zdroj: *Vlastní zpracování*

4.6.4 Resumé výsledků dotazníkového šetření

V níže uvedeném textu jsou shrnuty podstatné skutečnosti vyplývající z realizovaného dotazníkového šetření:

- Všichni dotazovaní elektronický podpis znají
- V rámci svého zaměstnání jej využívá naprostá většina
- Při své každodenní práci jej využívá větší polovina respondentů
- Shodující odpovědi většiny dotazovaných na otázku při jaké činnosti využívají elektronický podpis v zaměstnání, byly následující:
  - při vyhotovení dokumentů
  - při zasílání korespondence mezi úřady

- po každém vyhotovení spisu v elektronické podobě (před jeho odesláním)

- Drtivá většina dotazovaných uvádí, že elektronický podpis využívá v rámci své pracovní činnosti 1 – 3 roky

- Jak uvádí analýza, před užíváním elektronického podpisu proběhlo školení zaměstnavatelem

- Téměř všichni dotazovaní vědí, že doba platnosti elektronického podpisu je časově omezena

- Jak je již zmíněno v úvodu čtvrté kapitoly na Okresním soudě v Ostravě jsou využívány dva kvalifikované certifikáty pro aplikaci elektronického podpisu, které vydávají První certifikační autorita, a.s. a Česká pošta, s.p. Tento fakt potvrdila čtvrtina respondentů, zbytek uvedl jednu ze dvou zmíněných variant.

- V rámci soukromého života elektronický podpis využívá menší čtvrtina z respondentů.

- Největší výhody v užívání elektronického podpisu spatřují dotazovaní především ve větší bezpečnosti v rámci elektronické komunikace a úspoře času.

- Naopak negativa jsou shledávána hlavně v omezené platnosti certifikátu a nedůvěře v elektronickou komunikaci.

- Dle názoru dotazovaných, veřejnost není dostatečně obeznámena s elektronickým podpisem a možnostmi jeho využití.

4.6.5 Návrhy a doporučení

V následující kapitole se budu snažit Okresnímu soudu v Ostravě navrhnout několik doporučení, která by mohla vést ke zkvalitnění úrovně využití elektronického podpisu v této instituci.

Dle analýzy méně než jedna čtvrtina respondentů ví, které dvě certifikační autority poskytují kvalifikované certifikáty pro Okresní soud v Ostravě. Pro osvěžení si informací či upozornění na nové změny v zákoně o elektronickém podpise bych provedl školení, které bych opakoval co dva roky.

Taktéž bych doporučil zveřejnit na internetových stránkách Okresního soudu v Ostravě rozsáhlejší informace týkající se elektronického podpisu, neboť z uvedených informací není patrné, že kvalifikovaný certifikát pro analyzovanou instituci poskytují dvě certifikační autority (První certifikační autorita, a.s. a Česká pošta, s. p.). Dle publikovaných informací se jedná pouze o 1. CA, a.s.

Je nesporné, že využíváním elektronických podatelen byla dosažena úspora jak časová, tak finanční – z důvodu ušetření provozních nákladů (není již nutné zasílat dokumenty prostřednictvím klasické pošty, tudíž se ušetří za známky, obálky apod.). Agenda řešena elektronicky občanům také odpouští správní poplatky, což může znamenat úsporu až stovek korun

Díky tomuto faktu bych doporučil certifikačním autoritám, které poskytují certifikáty, aby snížily pořizovací cenu certifikátů a tudíž podporovaly využívání elektronického podpisu u široké veřejnosti. Tato skutečnost by mohla vést k tomu, že datovou schránku si začne pořizovat větší počet fyzických osob a stoupne tak komunikace mezi občany a úřady v elektronické podobě, čímž opět klesnou náklady za známky, obálky a zároveň bude tento krok mít pozitivní ekologický efekt, neboť se ušetří značné množství papírů.

Všeobecným doporučením ke zkvalitnění bezpečnosti využívání elektronického podpisu by bylo řešení v podobě kvalitního antivirového programu jak už u všech státních institucí tak fyzických osob. Především fyzické osoby často využívají volně dostupné antivirové programy, které jsou zdarma k dispozici na internetových portálech.

Doporučil bych zakoupit pro bezpečnou elektronickou komunikaci kvalitní antivirový program např. AVG internet security 2011 či NOD32.

V této kapitole jsem se zabýval využitím elektronického podpisu v praxi. Věnoval jsem se podstatným tématům, která jsou spojená s využitím elektronického podpisu na Okresním soudě v Ostravě. Zároveň jsem v této části práce zmínil potenciální problémy spojené s elektronickým podpisem a možné způsoby řešení. V rámci této předposlední kapitoly jsem také provedl analýzu využití elektronického podpisu prostřednictvím dotazníkového šetření. Na základě výsledků dotazníkového šetření jsem vypracoval návrhy a doporučení pro zkvalitnění úrovně využití elektronického podpisu na Okresním soudě v Ostravě.

5. Závěr

Hlavní cíl, který jsem si v úvodu této diplomové práce stanovil, jsem splnil. Zhodnotil jsem nejen úroveň využití elektronického podpisu na Okresním soudě v Ostravě, ale také prostudoval právní úpravu elektronického podpisu, jenž je nezbytná pro správné užívání elektronického podpisu v této instituci. Následně jsem také zanalyzoval samotné využití elektronického podpisu v praxi.

Diplomovou práci jsem rozdělil do pěti kapitol. Po úvodu jsem se zabýval teoretickými východisky využití elektronického podpisu, kdy jsem čtenáři přiblížil podstatné informace týkající se elektronického podpisu.

Ve třetí kapitole jsem se věnoval právní úpravě elektronického podpisu, jelikož znalost popsaných právních předpisů je nezbytná pro správné užívání elektronického podpisu na Okresním soudě v Ostravě.

Ve čtvrté kapitole jsem se zaměřil na samotné využití elektronického podpisu v praxi a na potenciální problémy spojené s elektronickým podpisem. Poté co jsem věnoval pozornost důležitým tématům a dokumentům, které jsou nezbytné pro řádné fungování elektronického podpisu v praxi, zaměřil jsem se na analýzu využití elektronického podpisu na Okresním soudě v Ostravě.

Z analýzy, kterou jsem provedl prostřednictvím dotazníkového šetření, vyplynulo, že zaměstnanci elektronický podpis znají a v rámci svého zaměstnání jej využívá naprostá většina z nich a to nejčastěji při každodenní práci.

Analýza dále ukázala, že před samotným užíváním elektronického podpisu proběhlo školení zaměstnavatelem. Podstatným zjištěním byla skutečnost, že pouze jedna čtvrtina dotazovaných ví, které dvě certifikační autority poskytují kvalifikované certifikáty pro tuto instituci. Z tohoto důvodu jsem doporučil školení zaměstnanců, kteří by si nejen osvěžili informace, ale mohly by být upozornění na nové změny v zákoně o elektronickém podpisu.

Prostřednictvím dotazníkového šetření jsem se rovněž dozvěděl, že elektronický podpis využívá v rámci svého soukromého života menší čtvrtina oslovených zaměstnanců.

Za tímto faktem mohou být negativa, které zaměstnanci především spatřují ve využívání elektronického podpisu. Jedná se o omezenou platnost certifikátu a nedůvěru v elektronickou komunikaci.

Myslím si, že elektronický podpis lze považovat za kvalitní komunikační nástroj. Jestliže tomu tak má být i nadále, je potřeba odstranit současná negativa a zaměřit se na propagaci elektronického podpisu vůči široké veřejnosti. Jestliže se poučený uživatel orientuje v procedurách spojených s užíváním párových dat a má vhodnou aplikaci, přináší mu pak tato technologie více výhod nežli nevýhod.

Za přínos této práce považuji zhodnocení úrovně využití elektronického podpisu na Okresním soudě v Ostravě. Jelikož u této instituce problematika elektronického podpisu nebyla doposud řešena, vidím využití této práce v možnosti aplikace doporučení, které jsem navrhl na základě výsledků z dotazníkového šetření. Především se jedná o školení zaměstnanců, neboť dochází nejen ke změnám legislativy, ale také ke změnám v oblasti samotného využití elektronického podpisu v praxi.

Seznam použité literatury

Monografie

[1] BOSÁKOVÁ, D. a kol. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. 141 s. ISBN 80-7263-125-X.

[2] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. 157 s. ISBN 978-80-7263-465-1.

[3] REICHEL, J. *Kapitoly metodologie sociálních výzkumů*. 1. vyd. Praha: Grada Publishing, 2009. 189 s. ISBN 978-80-247-3006-6.

[4] SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systémů*. 2.vyd.Praha: C.H. Beck, 2004. 770 s. ISBN 80-7179-765-0.

[5] ZELENKA, J. a kol. *Ochrana dat: kryptologie.* 1.vyd. Hradec Králové: Gaudeamus, 2003. 198 s. ISBN 80-7041-737-4.

Právní předpisy

[6] Nařízení vlády č.495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů

[7] Směrnice 1999/93/EC Evropského parlamentu a Rady o zásadách společenství pro elektronické podpisy

[8] Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb

[9] Vyhláška č. 496/2004 Sb., o elektronických podatelnách

[10] Zákon č. 40/1964 Sb., občanský zákoník

[11] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů

Internetové články

[12] DOLEŽAL, D. Co to je digitální certifikát. *E-komerce* [online]. 2003 [cit. 2011-02-16]. Dostupný z WWW: <http://interval.cz/clanky/co-to-je-digitalni-certifikat/>.

[13] GOTWALDOVÁ, D. Pravidla pro zajištění provozu ePodatelny. *Justice* [online]. 2010 [cit. 2011-03-29]. Dostupný z WWW:<http://portal.justice.cz/Justice2 /Soud/soud.aspx?o=157&j=167&k=1610&d=191378/>.

[14] SMEJKAL, V. Datové schránky nastupují. *IHNED* [online]. 2009 [cit. 2011-04-01]. Dostupný z WWW: <http://pravniradce.ihned.cz/c1-37865170-datove-schranky-nastupuji/>.

[15] STAŇKOVÁ, M. Počty nevyřízených věcí se snižují. *Zpravodajský měsíčník pro státní správu a podnikatele* [online]. 2008 [cit. 2011-03-28]. Dostupný z WWW: <http://www.parlament-vlada.cz/modules.php?name=News&file=print&sid=504/>.

[16] ŽIŽLAVSKÁ, V. Datové schránky – justice. *Mediafax* [online]. 2010 [cit. 2011-03-28]. Dostupný z WWW:<http://www.mediafax.cz/domaci/3004277-Datovymi-schrankami-ktere-vyuziva-ceska-justice-jiz-prosly-vice-nez-dva-miliony-zprav/>.

Internetové zdroje

[17] *I. CA a.s.* [online]. 2011 [cit. 2011-03-19]. Dostupný z WWW: <http://www.ica.cz/cz/menu/1/obecne-informace/ >.

[18] *e-Government* [online]. 2011 [cit. 2011-03-17]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/micr/egovernment/default.htm>.

[19] *eIdentity* [online]. 2010 [cit. 2011-03-29]. Dostupný z WWW: <https://www.eidentity.cz/app/>.

[20] *ePodatelna* [online]. 2008 [cit. 2011-03-28]. Dostupný z WWW: <http://obcanskyzakonik.justice.cz/ejustice/epodatelna.html/ >.

[21] *Informace k používání elektronického podpisu* [online]. 2010 [cit. 2011-03-25]. Dostupný z WWW: <http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho podpisu.aspx>.

[22] *Kvalifikovaná certifikační autorita* [online]. 2011 [cit. 2011-03-17]. Dostupný z WWW:<http://www.cpost.cz/cz/sluzby/e-sluzby/kvalifikovana-certifikacni-autorita-id287/>.

[23] *Kvalifikované časové razítko* [online]. 2009 [cit. 2011-03-20]. Dostupný z WWW: <http://www.aipsafe.cz/cs/datove-schranky/pojmy/kvalifikovane-casove-razitko/>.

[24] *Příručka Certifikační autority PostSignum* [online]. 2010 [cit. 2011-03-16]. Dostupný z WWW: <http://www.postsignum.cz/files/navody/CA_P54_zakaznik_PO_PFO.pdf/>.

[25] *Příručka o elektronickém podpisu* [online]. 2007 [cit. 2011-03-15]. Dostupný z WWW:<http://aplikace.mvcr.cz/archiv2008/micr/files/3908/prirucka_el_podpis.pdf/>.

[26] *Uživatelská příručka ePodatelny* [online]. 2010 [cit. 2011-03-28]. Dostupný z WWW: <http://epodatelna.justice.cz/ePodatelna/epo1200new/form.do/ >.

[27] *Veřejná správa* [online]. 2011 [cit. 2011-03-18]. Dostupný z WWW: <http://www.risy.cz/cs/krajske-ris/stredocesky-kraj/verejna-sprava/>.

[28] *Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb* [online]. 2010 [cit. 2011-03-23]. Dostupný zWWW:<http://www.mvcr.cz/clanek/vyhlaska-c-378-2006-sb-o-postupech-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb.aspx/ >.

[29] *Zákon č. 227/2000 Sb., o elektronickém podpisu* [online]. 2010 [cit. 2011-03-21]. Dostupný z WWW: <http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx/ >.

[30] *Změny v systému doručování v resortu justice* [online]. 2009 [cit. 2011-03-29]. Dostupný z WWW:<http://portal.justice.cz/Justice2/MS/ms.aspx?j=33&o=23&k=5208&d=308460/ >.

[31] *Zřízení elektronického podpisu* [online]. 2011 [cit. 2011-03-22]. Dostupný z WWW:<http://www.proconsulting.cz/elektronickypodpis.html?utm_source=Seznam&utm_medium=Sklik&utm_campaign=elektronicky_podpis>.

Seznam zkratek

CA – certifikační autorita

I. CA – První certifikační autorita, a.s.

CRL – seznam zneplatněných certifikátů

MSp - Ministerstvo spravedlnosti

s. p. – státní podnik

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že jeden výtisk diplomové práce bude uložen v Ústřední knihovně VŠB-TUO k prezenčnímu nahlédnutí a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne ……

……
jméno a příjmení studenta

Adresa trvalého pobytu studenta:

…….

Seznam příloh

Příloha číslo I.

Dotazník

Vážená paní, vážený pane,

při zpracování diplomové práce týkající se využití elektronického podpisu na Okresním soudě v Ostravě se na Vás obracím s prosbou o spolupráci.
Chtěl bych Vás požádat o vyplnění níže uvedeného dotazníku. Účelem tohoto dotazníku je zhodnotit úroveň využití elektronického podpisu na Okresním soudě v Ostravě.

Dotazník je anonymní a bude sloužit pouze pro potřeby této diplomové práce.
Za vyplnění dotazníku Vám děkuji.

Bc. Ondřej Kyčerka
student EkF, VŠB – TU Ostrava

1. Víte co je to elektronický podpis?

□ ano □ ne

2. Využíváte elektronický podpis v rámci svého zaměstnání? Pokud ne, přejděte prosím na otázku č. 7.

□ ano □ ne

3. Jak často elektronický podpis využíváte?

□ denně

□ minimálně 1x za 14 dní

□ alespoň 1x měsíčně

4. Uveďte, při jaké specifické činnosti využíváte elektronický podpis při zaměstnání?

……

……

5. Jak dlouho již v rámci své pracovní činnosti elektronický podpis využíváte?

□ méně než 1 rok □ 1-3 roky □ více než 3 roky

6. Byli jste před užíváním elektronického podpisu proškoleni zaměstnavatelem?

□ ano □ ne

7. Víte, že doba platnosti elektronického podpisu je časově omezena?

□ ano □ ne

8. Víte, která z uvedených certifikačních autorit poskytuje kvalifikovaný certifikát pro využívání elektronického podpisu na Okresním soudě v Ostravě?

□ První certifikační autorita, a.s.

□ Česká pošta, s.p.

□ eIdentity, a.s.

9. Využíváte elektronický podpis v osobním životě?

□ ano □ ne

10. Jaké výhody spatřujete ve využívání elektronického podpisu?

□ úspora času

□ větší bezpečnost v rámci elektronické komunikace

□ nenapodobitelnost podpisu

□ jiné, prosím uveďte

……..

11. Jaké nevýhody spatřujete ve využívání elektronického podpisu?

□ vysoké náklady

□ omezená platnost certifikátu

□ nedůvěra v elektronickou komunikaci

□ jiné, prosím uveďte

…….....

12. Domníváte se, že veřejnost zná elektronický podpis a možnosti jeho využití?

□ ano □ ne

13. Jste muž nebo žena?

□ muž □ žena

14. Kolik je Vám let?

□ 18-30 let

□ 31-40 let

□ 41-50 let

□ 51-60 let

□ více než 61 let